目　录

第1章 相关知识回顾

本章复习数论、单位复根和集合论基础的一些熟知内容，大多数证明只有概要.

1.1 数论

首先讨论数学归纳法. 回顾**自然数集**$\mathbb{N}$是由

$$\mathbb{N} = \{\text{整数 } n : n \geqslant 0\}$$

定义的，即$\mathbb{N}$是一切非负整数的集合. 数学归纳法是基于$\mathbb{N}$的下列性质的一种证明方法：

最小整数公理[⊖] *在$\mathbb{N}$的每个非空子集C中都有最小整数.*

假定公理成立则对于任意固定的、可以是负的整数m，每个大于或等于m的整数集合C都有最小整数. 如果$m \geqslant 0$，它就是最小整数公理. 如果$m<0$，则$C \subseteq \{m, m+1, \cdots, -1\} \cup \mathbb{N}$且

$$C = (C \cap \{m, m+1, \cdots, -1\}) \cup (C \cap \mathbb{N}).$$

如果有限集$C \cap \{m, m+1, \cdots, -1\} \neq \varnothing$，则它包含一个最小整数，显然该数就是$C$中的最小整数；如果$C \cap \{m, m+1, \cdots, -1\} = \varnothing$，则$C$包含在$\mathbb{N}$中，最小整数公理保证$C$有最小整数.

定义 *自然数p为**素数**，如果$p \geqslant 2$且没有因数分解$p = ab$，其中$a < p, b < p$为自然数.*

1

命题 1.1 *每个自然数$n \geqslant 2$不是素数就是素数的乘积.*

证明 设C是由一切大于1的、不满足该性质的自然数组成的集合$\mathbb{N}$的子集，要证$C = \varnothing$. 如果C非空，则它含有最小整数，譬如说m. 因$m \in C$，所以m不是素数，从而有自然数a和b使得$m = ab, a < m$和$b < m$. 由于a和b都比m小，而m是C中的最小整数，因此两者都不在C中，所以它们的每一个或者是素数，或者是素数的乘积，由此$m = ab$是素数（至少两个）的乘积，这与m不满足本命题相矛盾. ■

有两种归纳法.

定理 1.2（数学归纳法） *设m是固定的整数，且对每个整数$n \geqslant m, S(n)$是一个命题. 如果*

（i）$S(m)$真，且

（ii）$S(n)$真蕴涵$S(n+1)$真，

则对所有整数$n \geqslant m, S(n)$都真.

证明 设C是一切使得$S(n)$不真的整数$n \geqslant m$的集合，如果C空，定理已得到证明. 否则，在C中有最小整数k，由（i），$k > m$，因而存在命题$S(k-1)$. 因为k是C中的最小整数，所以$k-1 < k$蕴涵$k-1 \notin C$. 于是，$S(k-1)$为真. 由（ii），$S(k) = S([k-1]+1)$也为真，这与$k \in C$矛盾（$S(k)$是C中的命题，故为假）. ■

定理 1.3（第二归纳法） *设m是固定的整数，且对每个整数$n \geqslant m, S(n)$是一个命题. 如果*

（i）$S(m)$真，且

（ii）如果对一切满足$m \leqslant k < n$的$k, S(k)$真，则$S(n)$本身也真，

则对所有整数$n \geqslant m, S(n)$都真.

⊖ 该性质通常称为良序原则.

证明概要 与第一归纳法的证明类似. ■

现在回顾初等数论的一些结果.

定理 1.4（带余除法） 给定整数 a,b，其中 $a\neq 0$，存在唯一的整数 q 和 r 使得

$$b=qa+r, 0\leqslant r<|a|.$$

证明概要 考虑一切形如 $b-na$ 的非负整数，其中 $n\in \mathbb{Z}$. 定义 r 为形如 $b-na$ 的最小非负整数，并令 q 为出现在表达式 $r=b-na$ 中的整数 n.

如果 $qa+r=q'a+r'$，其中 $0\leqslant r'<|a|$，则 $|(q-q')a|=|r'-r|$. 现在 $0\leqslant|r'-r|<|a|$，

[2] 如果 $|q-q'|\neq 0$，则有 $|(q-q')a|\geqslant|a|$. 由此可知，等式两端都为0，即 $q=q'$ 和 $r=r'$. ■

定义 如果 a 和 b 都是整数且 $a\neq 0$，则称带余除法中的 q 和 r 为 a 除 b 的**商**和**余数**.

注 特别地，当 b 为负数时带余除法也有意义. 粗心人会以为 b 和 $-b$ 除以 a 有相同的余数，这通常是错的. 例如7除60和-60，

$$60=7\cdot 8+4 \text{ 和 } -60=7\cdot(-9)+3$$

由此，7除60和-60的余数是不同的.

系 1.5 有无限个素数.

证明（欧几里得） 假设只有有限个素数，它们是 $p_1,p_2,\cdots,p_k$. 令 $M=(p_1\cdots p_k)+1$. 由命题1.1，M 不是素数就是素数的乘积，但 M 既不是素数（对每个 i，$M>p_i$）也没有素因子 p_i，因为 p_i 除 M 得余数1而不是0，例如，p_1 除 M 得 $M=p_1(p_2\cdots p_k)+1$，商 $q=p_2\cdots p_k$，余数 $r=1$；p_2 除 M 得 $M=p_2(p_1p_3\cdots p_k)+1, q=p_1p_3\cdots p_k, r=1$；等等. 这一矛盾证明不可能只有有限个素数，从而必有无限个. ■

定义 设 a 和 b 都是整数，如果存在整数 d 使得 $b=ad$，则称 a 是 b 的**因数**. 也称 a **整除** b 或 b 是 a 的**倍数**，记为

$$a\mid b.$$

下面要转移我们的视点. 在开始学习长除法的时候，强调商 q，而余数 r 不过是丢弃的零头. 这里关注给定的数 b 是否为数 a 的倍数，而究竟多少倍是次要的. 因此，从现在起要强调余数. 于是 $a\mid b$ 当且仅当 b 除以 a 得余数 $r=0$.

定义 整数 a 和 b 的**公因数**是指满足 $c\mid a$ 和 $c\mid b$ 的整数 c. a 和 b 的**最大公因数**或 gcd 记为 (a,b)，定义如下：

$$(a,b)=\begin{cases}0, & \text{如果 } a=0=b\\ a\text{ 和 }b\text{ 公因数中的最大者}, & \text{其他}\end{cases}$$

命题 1.6 如果 p 是素数，b 是任一整数，则

$$(p,b)=\begin{cases}p, & \text{如果 } p\mid b\\ 1, & \text{其他}\end{cases}$$

[3] **证明概要** 一个正的公因数也是素数 p 的因数，因此不是 p 就是1. ■

定理 1.7 如果 a 和 b 是整数，则 $(a,b)=d$ 是 a 和 b 的线性组合，即存在整数 s 和 t 使得 $d=sa+tb$.

证明概要 设

$$I=\{sa+tb: s,t\in \mathbb{Z}\}$$

（包括正数和负数的一切整数的集合记为$\mathbb{Z}$）. 如果 $I\neq\{0\}$，令 d 为 I 中的最小正整数，作为 I

的成员，有整数 s 和 t 使得 $d=sa+tb$. 可以断定 $I=(d)$，(d) 是指 d 的一切倍数的集合. 显然，$(d)\subseteq I$. 对于反包含，取 $c\in I$，由带余除法，$c=qd+r$，其中 $0\leqslant r<d$. 如果 $r\neq 0$，则 $r=c-qd\in I$ 与 d 是最小相矛盾. 因此，$d\mid c$，$c\in(d)$ 且 $I=(d)$. 由此，d 是 a 和 b 的公因数且是最大的. ■

命题 1.8 设 a 和 b 都是整数，a 和 b 的非负公因数 d 是 gcd 当且仅当对每个公因数 c 有 $c\mid d$.

证明概要 如果 d 是 gcd，则 $d=sa+tb$，因此，如果 $c\mid a$ 且 $c\mid b$，则 $c\mid sa+tb=d$. 反之，如果 d 是公因数且对每个公因数 c 有 $c\mid d$，则对所有的 c 有 $c\leqslant d$，因此 d 是最大的. ■

系 1.9 设 I 是 $\mathbb{Z}$ 的子集满足

(ⅰ) $0\in I$；

(ⅱ) 如果 a，$b\in I$，则 $a-b\in I$；

(ⅲ) 如果 $a\in I$ 且 $q\in\mathbb{Z}$，则 $qa\in I$.

则存在自然数 $d\in I$ 使得 I 由 d 的一切倍数组成.

证明概要 这正是用来证明定理 1.7 的子集 I 所具备的性质. ■

定理 1.10（欧几里得引理） 如果 p 是素数且 $p\mid ab$，则 $p\mid a$ 或 $p\mid b$. 更一般地，如果素数 p 整除乘积 $a_1a_2\cdots a_n$，则 p 至少整除其中的一个因数 a_i.

证明概要 如果 $p\nmid a$，则 $(p,a)=1$ 且 $1=sp+ta$. 因此，$b=spb+tab$ 是 p 的倍数. 第二个结论可对 $n\geqslant 2$ 用归纳法证明. ■

定义 称整数 a 和 b **互素**，如果它们的 $\gcd(a,b)=1$.

系 1.11 设 a，b 和 c 都是整数. 如果 c 和 a 互素且 $c\mid ab$，则 $c\mid b$.

证明概要 因为 $1=sc+ta$，所以有 $b=scb+tab$. ■ [4]

命题 1.12 如果 p 是素数，则 $p\mid\binom{p}{j}$，其中 $0<j<p$.

证明概要 由二项式系数的定义，$\binom{p}{j}=p!/j!(p-j)!$，于是

$$p!=j!(p-j)!\binom{p}{j}.$$

根据欧几里得引理，$p\nmid j!(p-j)!$ 蕴涵 $p\mid\binom{p}{j}$. ■

命题 1.13 (ⅰ) 如果 a 和 b 都是整数，则 a 和 b 互素当且仅当存在整数 s 和 t 使得 $1=sa+tb$.

(ⅱ) 如果 $d=(a,b)$，其中 a 和 b 不全为 0，则 $(a/d,b/d)=1$.

证明 (ⅰ) 由定理 1.7 得必要性. 对于充分性，注意到 1 是最小正整数，因而此时 1 是 a 和 b 的最小正线性组合，从而 $(a,b)=1$. 或者用另一种证法，如果 c 是 a 和 b 的公因数，则 $c\mid sa+tb$，因此 $c\mid 1$，从而 $c=\pm 1$.

(ⅱ) 因 d 是公因数，所以 $d\neq 0$ 且 a/d 和 b/d 是整数. 等式 $d=sa+tb$ 导出 $1=s(a/d)+t(b/d)$，根据 (ⅰ)，$(a/d,b/d)=1$. ■

下面的结果给出求两整数 gcd 的具体方法，同时可把它表示为线性组合.

定理 1.14（欧几里得算法） 设 a 和 b 都是正整数. 存在算法求它们的 $\gcd, d=(a,b)$，且存在算法求整数对 s 和 t 满足 $d=sa+tb$.

注 详情可见定理 3.40 对多项式的证明.

要知道希腊人如何发现该结果，见 Rotman 所著的《A First Course in Abstract Algebra》49 页关于 antanairesis 的讨论.

证明概要 辗转相除如下：开始 $b=qa+r$，其中 $0\leqslant r<a$. 第二步 $a=q'r+r'$，其中 $0\leqslant r'<r$. 再下一步 $r=q''r'+r''$，其中 $0\leqslant r''<r'$，等等. 最终该步骤停止，而最后的余数就是 gcd. 从最后的等式倒推，可把 gcd 表示为 a 和 b 的线性组合. ■

5

命题 1.15 如果 $b\geqslant 2$ 是整数，则每个正整数 m 都有一个底数为 b 的表达式：存在整数 d_i 满足 $0\leqslant d_i<b$，使得

$$m=d_kb^k+d_{k-1}b^{k-1}+\cdots+d_0;$$

此外，如果 $d_k\neq 0$，则该表达式唯一.

证明概要 由最小整数公理，存在整数 $k\geqslant 0$ 使得 $b^k\leqslant m<b^{k+1}$，又由带余除法，$m=d_kb^k+r$，其中 $0\leqslant r<b^k$. 对 $m\geqslant 1$ 用归纳法可证明各 b-进位数字的存在性. 唯一性也可以对 m 作归纳证明，但要注意一切可能产生的情形. ■

称数 d_k，d_{k-1}，…，d_0 为 m 的 **b-进位数字**.

定理 1.16（算术基本定理） 假定整数 $a\geqslant 2$ 有因数分解

$$a=p_1\cdots p_m \text{ 和 } a=q_1\cdots q_n,$$

其中所有的 p 和所有的 q 都是素数. 则 $n=m$ 且各个 q 可以重新标号使得对一切 i 有 $q_i=p_i$. 因此存在唯一的互不相同的素数 p_i 和唯一的 n 个整数 $e_i>0$ 使得

$$a=p_1^{e_1}\cdots p_n^{e_n}.$$

证明 对 m 和 n 的大者 ℓ 用归纳法证明本定理.

如果 $\ell=1$，则给出的等式为 $a=p_1=q_1$，结论显然成立. 关于归纳步，注意给出的等式表明 $p_m\mid q_1\cdots q_n$. 由欧几里得引理，必有某个 i 使得 $p_m\mid q_i$. 但 q_i 是素数，除 1 和它自身外没有正因数，所以 $q_i=p_m$. 重新标号后，可以假定 $q_n=p_m$. 消去 p_m 得 $p_1\cdots p_{m-1}=q_1\cdots q_{n-1}$. 由归纳假设，$n-1=m-1$ 且对所有 q 重新标号后，对一切 i 有 $q_i=p_i$. ■

定义 整数 a 和 b 的**公倍数**是指满足 $a\mid c$ 和 $b\mid c$ 的整数 c. a 和 b 的**最小公倍数**或 lcm 记为 $[a,b]$，定义如下：

$$[a,b]=\begin{cases}0, & \text{如果 } a=0=b\\ a\text{ 和 }b\text{ 的最小正公倍数}, & \text{其他}\end{cases}$$

命题 1.17 设 $a=p_1^{e_1}\cdots p_n^{e_n}$ 和 $b=p_1^{f_1}\cdots p_n^{f_n}$，其中对一切 i，$e_i\geqslant 0$，$f_i\geqslant 0$；令

$$m_i=\min\{e_i,f_i\},M_i=\max\{e_i,f_i\}.$$

则 a 和 b 的 gcd 和 lcm 为

$$(a,b)=p_1^{m_1}\cdots p_n^{m_n} \text{ 和} [a,b]=p_1^{M_1}\cdots p_n^{M_n}.$$

6

证明概要 $p_1^{e_1}\cdots p_n^{e_n}\mid p_1^{f_1}\cdots p_n^{f_n}$ 当且仅当对一切 i，$e_i\leqslant f_i$. ■

定义 固定 $m\geqslant 0$. 如果 $m\mid(a-b)$ 则称整数 a 和 b **对模 m 同余**，记为

$$a\equiv b \bmod m.$$

命题 1.18 设 $m\geqslant 0$ 是固定的整数，则对所有整数 a，b，c，

（i）$a\equiv a \bmod m$；

（ii）如果 $a\equiv b \bmod m$，则 $b\equiv a \bmod m$；

（iii）如果 $a\equiv b \bmod m$ 且 $b\equiv c \bmod m$，则 $a\equiv c \bmod m$.

注 （i）说明同余是**自反的**，（ii）说明同余是**对称的**，（iii）说明同余是**传递的**.

证明概要 所有结论容易从同余的定义得出. ■

命题 1.19 设 $m \geqslant 0$ 是固定的整数.

（i）如果 $a = qm + r$，则 $a \equiv r \bmod m$.

（ii）如果 $0 \leqslant r' < r < m$，则 $r \not\equiv r' \bmod m$；即 r 和 $r' \bmod m$ 不同余.

（iii）$a \equiv b \bmod m$ 当且仅当 m 除 a 和 m 除 b 的余数相等.

（iv）如果 $m \geqslant 2$，则每个整数 a 恰和 $0, 1, \cdots, m-1$ 之一对模 m 同余.

证明概要 （i）和（iii）是简单事实；（ii）只需注意 $0 < r' - r < m$ 就可推出，而（iv）由（i）和（ii）推出. ■

下面的结果表明同余与加法相容，同余与乘法也相容.

命题 1.20 设 $m \geqslant 0$ 是固定的整数.

（i）如果 $a \equiv a' \bmod m$ 且 $b \equiv b' \bmod m$，则

$$a + b \equiv a' + b' \bmod m.$$

（ii）如果 $a \equiv a' \bmod m$ 且 $b \equiv b' \bmod m$，则

$$ab \equiv a'b' \bmod m.$$

（iii）如果 $a \equiv b \bmod m$，则对一切 $n \geqslant 1$，$a^n \equiv b^n \bmod m$.

证明概要 命题显然成立. ■

7

先前 7 除 60 和 -60 分别得到余数 4 和 3，而 $4+3=7$，这不是偶然的巧合. 如果 a 是整数且 $m \geqslant 0$，设 $a \equiv r \bmod m$ 且 $-a \equiv r' \bmod m$，则由上面的命题得到

$$0 = -a + a \equiv r' + r \bmod m.$$

下面的例子说明怎样运用同余. 在每种情形下，关键是要在解题时用余数代替该数.

例 1.21 （i）证明：如果 a 是 $\mathbb{Z}$ 中的数，则 $a^2 \equiv 0, 1$，或 $4 \bmod 8$.

如果 a 是整数，则 $a \equiv r \bmod 8$，其中 $0 \leqslant r \leqslant 7$；又由命题1.20（iii），$a^2 \equiv r^2 \bmod 8$. 因此只需观察余数的平方.

表 1.1 平方 mod8

r	0	1	2	3	4	5	6	7
r^2	0	1	4	9	16	25	36	49
$r^2 \bmod 8$	0	1	4	1	0	1	4	1

从表 1.1 可知，8 除一个完全平方数其余数只能是 0，1 或 4.

（ii）证明 $n = 1\,003\,456\,789$ 不是完全平方数.

因为 $1\,000 = 8 \cdot 125$，有 $1\,000 \equiv 0 \bmod 8$，所以

$$n = 1\,003\,456\,789 = 1\,003\,456 \cdot 1\,000 + 789 \equiv 789 \bmod 8.$$

8 除 789 得余数 5，于是 $n \equiv 5 \bmod 8$. 如果 n 是完全平方数，则 $n \equiv 0, 1$ 或 $4 \bmod 8$.

（iii）如果 m 和 n 是正整数，是否存在形如 $3^m + 3^n + 1$ 的完全平方数？

再来观察 mod8 的余数. $3^2 = 9 \equiv 1 \bmod 8$，由此可求得 $3^m \bmod 8$ 如下：如果 $m = 2k$，则 $3^m = 3^{2k} = 9^k \equiv 1 \bmod 8$；如果 $m = 2k+1$，则 $3^m = 3^{2k+1} = 9^k \cdot 3 \equiv 3 \bmod 8$. 于是

$$3^m = \begin{cases} 1 \bmod 8, & \text{如果 } m \text{ 是偶数;} \\ 3 \bmod 8, & \text{如果 } m \text{ 是奇数.} \end{cases}$$

用除以 8 的余数代替该数，根据 m 和 n 的不同配对，得到 3^m+3^n+1 的各种可能的余数：

$$3+1+1 \equiv 5 \bmod 8$$
$$3+3+1 \equiv 7 \bmod 8$$
$$1+1+1 \equiv 3 \bmod 8$$
$$1+3+1 \equiv 5 \bmod 8.$$

8

无论哪种情形余数都不是 0，1 或 4，因此由（i），形如 3^m+3^n+1 的数不可能是完全平方数. ■

命题 1.22 一正整数 a 被 3（或被 9）整除当且仅当它的各位（十进制）数字的和被 3（或被 9）整除.

证明概要 观察 $10^n \equiv 1 \bmod 3$（$10^n \equiv 1 \bmod 9$）. ■

命题 1.23 如果 p 是素数，a 和 b 是整数，则

$$(a+b)^p \equiv a^p + b^p \bmod p.$$

证明概要 运用二项式定理和命题 1.12. ■

定理 1.24（费马（Fermat）） 如果 p 是素数，则对 $\mathbb{Z}$ 中的每个 a，

$$a^p \equiv a \bmod p.$$

更一般地，对每个整数 $k \geqslant 1$，

$$a^{p^k} \equiv a \bmod p.$$

证明概要 如果 $a \geqslant 0$，对 a 用归纳法证明，其中归纳步运用命题 1.23. 第二个命题可对 $k \geqslant 1$ 用归纳法证明. ■

系 1.25 设 p 是素数，n 是正整数. 如果 $m \geqslant 0$ 且 Σ 是 m 的 p-进位各位数字之和，则

$$n^m \equiv n^{\Sigma} \bmod p.$$

证明概要 用底为 p 的指数表出 m，再用费马定理. ■

计算 7 除 10^{100} 的余数. 第一步，$10^{100} \equiv 3^{100} \bmod 7$. 第二步，因 $100 = 2 \cdot 7^2 + 2$，由上面的系得 $3^{100} \equiv 3^4 = 81 \bmod 7$. 因 $81 = 11 \times 7 + 4$，可得余数为 4.

定理 1.26 如果 $(a,m)=1$，则对每个整数 b，同余式

$$ax \equiv b \bmod m$$

关于 x 有解；事实上，$x=sb$ 就是一个解，其中 $sa \equiv 1 \bmod m$. 此外，任两个解关于模 m 同余.

证明概要 如果 $1=sa+tm$，则 $b=sab+tmb$. 因此 $b \equiv a(sb) \bmod m$. 又如果 $b \equiv ax \bmod m$，则

9

$0 \equiv a(x-sb) \bmod m$，所以 $m \mid a(x-sb)$. 因 $(m,a)=1$，由系 1.11，$m \mid (x-sb)$，因此 $x \equiv sb \bmod m$. ■

系 1.27 如果 p 是素数，a 不能被 p 整除，则同余式

$$ax \equiv b \bmod p$$

恒有解.

证明概要 如果 a 不能被 p 整除，则 $(a,p)=1$. ■

定理 1.28（孙子剩余定理） 如果 m 和 m' 互素，则下面两个同余式

$$x \equiv b \bmod m$$
$$x \equiv b' \bmod m'$$

有共解，且任两个解对模 mm' 同余.

证明概要 由定理 1.26，第一个同余式的解形如 $x=sb+km$，$k\in\mathbb{Z}$（其中 $1=sa+tm$）. 把它代入第二个同余式解 k. 另一种证法，存在整数 s 和 s' 使得 $1=sm+s'm'$，于是共解为

$$x = b'ms + bm's'.$$

为证唯一性，假定 $y\equiv b \bmod m$ 和 $y\equiv b' \bmod m'$，则 $x-y\equiv 0 \bmod m$ 和 $x-y\equiv 0 \bmod m'$，即 m 和 m' 都能整除 $x-y$，由习题 1.19 可得结论. ■

习题

1.1 证明 $1^2+2^2+\cdots+n^2=\frac{1}{6}n(n+1)(2n+1)=\frac{1}{3}n^3+\frac{1}{2}n^2+\frac{1}{6}n.$

1.2 证明 $1^3+2^3+\cdots+n^3=\frac{1}{4}n^4+\frac{1}{2}n^3+\frac{1}{4}n^2.$

1.3 证明 $1^4+2^4+\cdots+n^4=\frac{1}{5}n^5+\frac{1}{2}n^4+\frac{1}{3}n^3-\frac{1}{30}n.$

注：对 $k\geqslant 1$，把 $\sum_{i=1}^{n-1} i^k$ 表示成 n 的多项式的一般公式为

$$(k+1)\sum_{i=1}^{n-1} i^k = n^{k+1}+\sum_{j=1}^{k}\binom{k+1}{j}B_j n^{k+1-j};$$

系数中所含有理数 B_j ($j\geqslant 1$) 称为**伯努利**(Bernoulli) **数**，由

$$\frac{x}{e^x-1}=1+\sum_{j\geqslant 1}\frac{B_j}{j!}x^j$$

定义. 见 Borevich-Shafarevich 所著的《Number Theory》，382 页.

10

1.4 通过计算图 1.1 中边长为 $n+1$ 的正方形的面积 $(n+1)^2$，导出 $\sum_{i=1}^{n} i$ 的计算公式.

提示：对角线两侧三角形面积相等.

图 1.1

图 1.2

1.5 (i) 通过计算图 1.2 中底为 $n+1$ 高为 n 的长方形的面积 $n(n+1)$，导出 $\sum_{i=1}^{n} i$ 的计算公式.

(ii) (**阿尔哈森**(Alhazen)，约 965—1039) 对固定的 $k\geqslant 1$，用图 1.3 证明

$$(n+1)\sum_{i=1}^{n} i^k=\sum_{i=1}^{n} i^{k+1}+\sum_{i=1}^{n}\Big(\sum_{\ell=1}^{i}\ell^k\Big).$$

提示：如图 1.3，高为 $n+1$ 底为 $\sum_{i=1}^{n} i^k$ 的长方形可分成两部分，有阴影的台阶部分面积为 $\sum_{i=1}^{n} i^{k+1}$，

它上部的面积为

$$1^k+(1^k+2^k)+(1^k+2^k+3^k)+\cdots+(1^k+2^k+\cdots+n^k).$$

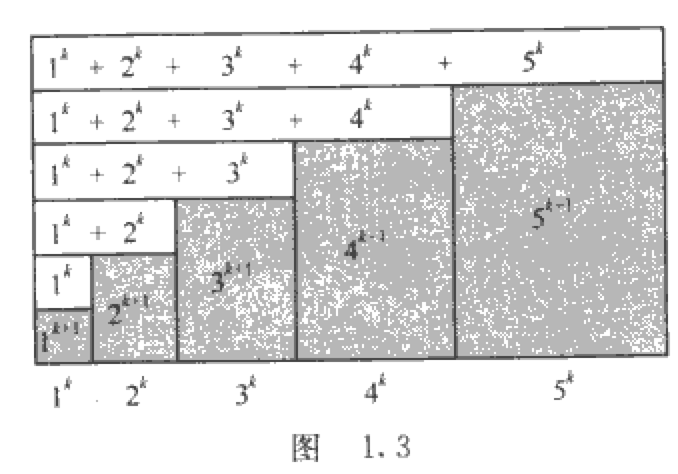


图 1.3

11

(ⅲ) 已知 $\sum_{i=1}^{n} i=\frac{1}{2}n(n+1)$，用 (ⅱ) 导出 $\sum_{i=1}^{n} i^2$ 的计算公式.

提示： 在阿尔哈森公式中，作代换 $\sum_{i=1}^{n}\left(\sum_{\ell=1}^{i} \ell\right)=\frac{1}{2}\sum_{i=1}^{n} i^2+\frac{1}{2}\sum_{i=1}^{n} i$，移项解出 $\sum_{i=1}^{n} i^2$.

1.6 (**莱布尼茨** (Leibniz)) 称函数 $f:\mathbb{R}\to\mathbb{R}$ 为 C^∞-**函数**，如果对每个自然数 n，存在 n 阶导数 $f^{(n)}$ (定义 $f^{(0)}$ 为 f). 如果 f 和 g 都是 C^∞-函数，证明

$$(fg)^{(n)}=\sum_{r=0}^{n}\binom{n}{r}f^{(r)}\cdot g^{(n-r)}.$$

1.7 (**双重归纳法**) 设 $S(m,n)$ 是一组有双重标号的命题，每个 $m\geqslant 1$ 和 $n\geqslant 1$ 对应一个命题. 假设

(ⅰ) $S(1,1)$ 为真；

(ⅱ) 如果 $S(m,1)$ 为真，则 $S(m+1,1)$ 为真；

(ⅲ) 如果 $S(m,n)$ 对所有 m 为真，则 $S(m,n+1)$ 对所有 m 为真.

证明对所有 $m\geqslant 1$ 和 $n\geqslant 1$，$S(m,n)$ 为真.

1.8 用双重归纳法证明对所有 $m,n\geqslant 1$，

$$(m+1)^n > mn.$$

1.9 证明 $\sqrt{2}$ 是无理数.

提示： 如果 $\sqrt{2}$ 是有理数，则 $\sqrt{2}=a/b$，且可假设 $(a,b)=1$ (事实上只要假定 a 和 b 至少有一个是奇数就够了). 取该等式的平方导出矛盾.

1.10 证明欧几里得定理的逆定理：如果整数 $p\geqslant 2$ 有如下性质，即它一旦整除一个乘积必整除因数之一，则该数是素数.

1.11 设 $p_1,p_2,p_3,\cdots$ 是由小到大的素数表：$p_1=2,p_2=3,p_3=5,\cdots$. 对 $k\geqslant 1$，令 $f_k=p_1p_2\cdots p_k+1$. 求使得 f_k 不是素数的最小 k.

提示： $19\mid f_7$，但 7 不是最小的 k.

1.12 如果 d 和 d' 是非零整数，且相互整除，证明 $d'=\pm d$.

1.13 证明每个正整数 m 可以写作 2 的不同幂的和.

提示： 用 2 为底数表示 m.

1.14 设 $(r,a)=1=(r',a)$，证明 $(rr',a)=1$.

1.15 (ⅰ) 证明：如果正整数 n **无平方因数** (即 n 不能被任何素数的平方整除)，则 $\sqrt{n}$ 是无理数.

(ⅱ) 证明整数 $m\geqslant 2$ 是完全平方数当且仅当它的每个素因数都出现偶数次.

1.16 证明$\sqrt[3]{2}$是无理数.

提示： 假定$\sqrt[3]{2}$能写作一个既约分数.

1.17 求 gcd$d = (12\ 327, 2\ 409)$，求整数 s 和 t 使得 $d=12\ 327s+2\ 409t$，并把分数 2 409/12 327 写作既约形式.

12

1.18 假定 $d=sa+tb$ 是整数 a 和 b 的线性组合，求出无限对整数 (s_k, t_k) 使得

$$d = s_k a + t_k b.$$

提示： 如果 $2s+3t=1$，则 $2(s+3)+3(t-2)=1$.

1.19 如果 a 和 b 互素且都能整除整数 n，则它们的积 ab 也能整除 n.

1.20 设 $a>0$，证明 $a(b,c)=(ab,ac)$. [必须假定 $a>0$，免得 $a(b,c)$ 为负.]

提示： 证明如果 k 是 ab 和 ac 的公因数，则 $k \mid a(b,c)$.

定义： 整数 $a_1, a_2, \cdots, a_n$ 的**公因数**是指对所有 i 有 $c \mid a_i$ 的整数 c；称最大的一个公因数为**最大公因数**，记为 $(a_1, a_2, \cdots, a_n)$.

1.21 (i) 证明：如果 d 是 $a_1, a_2, \cdots, a_n$ 的最大公因数，则 $d=\sum t_i a_i$，其中对于 $1\leqslant i\leqslant n$，t_i 是$\mathbb{Z}$中的数.

(ii) 证明：如果 c 是 $a_1, a_2, \cdots, a_n$ 的一个公因数，则 $c \mid d$.

1.22 (i) 证明 a,b,c 的 gcd (a,b,c) 等于$(a,(b,c))$.

(ii) 计算 $(120,168,328)$.

1.23 **毕达哥拉斯三元组**是指有序正整数三元组 (a,b,c)，满足

$$a^2+b^2=c^2;$$

如果 $\gcd(a,b,c)=1$，则称它为**本原的**.

(i) 如果 $q>p$ 是正整数，证明

$$(q^2-p^2, 2qp, q^2+p^2)$$

是毕达哥拉斯三元组. [可以证明每个本原毕达哥拉斯三元组 (a,b,c) 都是这种形式.]

(ii) 证明毕达哥拉斯三元组 $(9,12,15)$ (它不是本原的) 不是 (i) 给出的形式.

(iii) 用能求平方根但只能显示 8 位数的计算器并用求出 q 和 p 的方法证明

$$(19\ 597\ 501, 28\ 397\ 460, 34\ 503\ 301)$$

是毕达哥拉斯三元组.

定义： $a_1, a_2, \cdots, a_n$ 的**公倍数**是指对一切 i 有 $a_i \mid m$ 的整数 m. 如果 $a_i\neq 0$ **最小公倍数**是最小的正公倍数，否则为 0，写作 lcm 并记为 $[a_1, a_2, \cdots, a_n]$.

1.24 证明整数 $M\geqslant 0$ 是 $a_1, a_2, \cdots, a_n$ 的 lcm 当且仅当它是 $a_1, a_2, \cdots, a_n$ 的一个公倍数且可整除一切其他公倍数.

1.25 设 $a_1/b_1, \cdots, a_n/b_n \in \mathbb{Q}$，其中对一切 i 有 $(a_i, b_i)=1$. 如果 $M=\operatorname{lcm}\{b_1, \cdots, b_n\}$，证明 $Ma_1/b_1, \cdots, Ma_n/b_n$ 的 gcd 是 1.

1.26 (i) 证明 $[a,b](a,b)=ab$，其中 $[a,b]$ 是 a 和 b 的最小公倍数.

提示： 如果 a 和 b 都不为 0，证明 $ab/(a,b)$ 是 a 和 b 的一个公倍数，它可整除 a 和 b 的每个公倍数 c. 或者用命题 1.17.

(ii) 给出一个 $[a,b,c](a,b,c)\neq abc$ 的例子.

13

1.27 (i) 用分解为素数的方法求 $\gcd(210,48)$.

(ii) 求 $(1\ 234, 5\ 678)$.

1.28 设 a 和 b 是正整数且 $(a,b)=1$，又设 ab 是平方数，证明 a 和 b 两者都是平方数.

提示： a 和 b 的素因数的集合不交.

1.29 设 $n=p^r m$，其中 p 是素数且不能整除整数 $m\geqslant 1$. 证明

$$p \nmid \binom{n}{p^r}.$$

提示：假定不成立，交错相乘，并运用欧几里得引理.

1.30 设 m 是正整数，m'是重排 m 的各位数字（十进制）而得的整数（例如取 $m=314\ 159, m'=539\ 114$）. 证明 $m-m'$是9的倍数.

1.31 证明正整数 n 可被11整除当且仅当它的各位数字的交错和被11整除（如果 a 的数字为 $d_k\cdots d_2d_1d_0$，则它的交错和为 $d_0-d_1+d_2-\cdots$）.

提示：$10\equiv -1 \bmod 11$.

1.32 (i) 证明 $10q+r$ 被7整除当且仅当 $q-2r$ 被7整除.

(ii) 给定具有十进位数字 $d_kd_{k-1}\cdots d_0$ 的整数 a，定义

$$a'=d_kd_{k-1}\cdots d_1-2d_0.$$

证明 a 被7整除当且仅当 $a', a'', a''', \cdots$ 之一被7整除.（例如 $a=65\ 464$，则 $a'=6\ 546-8=6\ 538, a''=653-16=637, a'''=63-14=49$，由此可知65 464被7整除.）

1.33 (i) 证明 $1\ 000\equiv -1 \bmod 7$.

(ii) 证明：如果 $a=r_0+1\ 000r_1+1\ 000^2r_2+\cdots$，则 a 被7整除当且仅当 $r_0-r_1+r_2-\cdots$被7整除.

注：习题1.32和1.33合在一起给出一个有效的方法去确定一个大数是否被7整除. 例如 $a=33\ 456\ 789\ 123\ 987$，则 $a\equiv 0 \bmod 7$ 当且仅当 $987-123+789-456+33=1\ 230\equiv 0 \bmod 7$. 由习题1.32，$1\ 230\equiv 123\equiv 6 \bmod 7$，因此 a 不能被7整除.

1.34 证明不存在整数 x，y 和 z 满足

$$x^2+y^2+z^2=999.$$

提示：用例1.21(i).

1.35 证明没有一个完全平方数 a^2 的最后两位数是35.

提示：如果 a^2 的最后一位数是5，则 $a^2\equiv 5 \bmod 10$；如果 a^2 的最后两位数是35，则 $a^2\equiv 35 \bmod 100$.

1.36 如果 x 是不被3整除的奇数，证明 $x^2\equiv 1 \bmod 4$.

1.37 证明：如果 p 是素数且 $a^2\equiv 1 \bmod p$，则 $a\equiv \pm 1 \bmod p$.

[14] **提示**：用欧几里得引理.

1.38 如果 $(a,m)=d$，证明 $ax\equiv b \bmod m$ 有解当且仅当 $d \mid b$.

1.39 解同余方程 $x^2\equiv 1 \bmod 21$.

提示：对 $21 \mid (a+1)(a-1)$ 用欧几里得引理.

1.40 解联立同余方程

(i) $x\equiv 2 \bmod 5$ and $3x\equiv 1 \bmod 8$；

(ii) $3x\equiv 2 \bmod 5$ and $2x\equiv 1 \bmod 3$.

1.41 (i) 证明对一切 a 和 b 以及一切 $n\geqslant 1$，有 $(a+b)^n\equiv a^n+b^n \bmod 2$.

提示：考虑 a 和 b 的奇偶性.

(ii) 证明 $(a+b)^2\not\equiv a^2+b^2 \bmod 3$.

1.42 一个荒芜的岛上，五个人和一只猴子白天采集椰子后都入睡了. 第一个人醒来决定要拿走他的份额. 他把椰子分成相等的五份还剩一只. 他把额外的一只给了猴子，藏好自己的一份，继续睡觉. 稍后，第二个人醒来，他把剩下的椰子又分成五份，发现又多了一只，他也把额外的一只给了猴子并拿走一份. 其余三人依次做了同样的事情. 求原先椰子的最小数目.

提示：试4只椰子.

1.2 单位根

先简单介绍一下复数$\mathbb{C}$. 定义复数 $z=a+ib$ 为平面上的点 (a,b)，称 a 为 z 的**实部**，b 为 z 的

虚部. $z=a+\mathrm{i}b=(a,b)$ 的模 $|z|$ 是指 z 到原点的距离：

$$|z|=\sqrt{a^2+b^2}.$$

命题 1.29（极式分解） 每个复数 z 都有因数分解

$$z=r(\cos\theta+\mathrm{i}\sin\theta),$$

其中 $r=|z|\geqslant 0$，$0\leqslant\theta<2\pi$.

证明 如果 $z=0$，则 $|z|=0$，θ 取任意值分解式都成立. 如果 $z=a+\mathrm{i}b\neq 0$，则 $|z|\neq 0$，因为

$$(a/|z|)^2+(b/|z|)^2=(a^2+b^2)/|z|^2=1,$$

所以 $z/|z|=(a/|z|,b/|z|)$. 因此存在角 θ（见图 1.4）使得 $z/|z|=\cos\theta+\mathrm{i}\sin\theta$，于是 $z=|z|(\cos\theta+\mathrm{i}\sin\theta)=r(\cos\theta+\mathrm{i}\sin\theta)$. ■

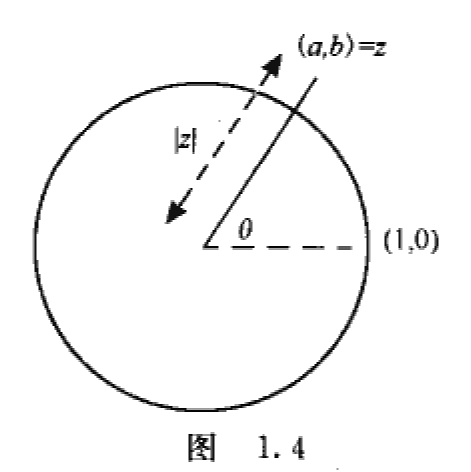


图 1.4

由此每个模 1 的复数 z 都是单位圆上的一个点，从而坐标为 $(\cos\theta,\sin\theta)$（因为 $\cos\theta=a/1$，$\sin\theta=b/1$，所以 θ 是从 x 轴到连接原点和 (a,b) 的直线的夹角）.

如果 $z=a+\mathrm{i}b=r(\cos\theta+\mathrm{i}\sin\theta)$，则 (r,θ) 是 z 的**极坐标**，这是命题 1.29 为什么叫做 z 的极式分解的理由.

在复数语言中，$\cos(\theta+\psi)$ 和 $\sin(\theta+\psi)$ 的三角和公式有一个有意义的解释.



命题 1.30（加法定理） 如果

$$z=\cos\theta+\mathrm{i}\sin\theta,\quad w=\cos\psi+\mathrm{i}\sin\psi,$$

则

$$zw=\cos(\theta+\psi)+\mathrm{i}\sin(\theta+\psi).$$

证明

$$\begin{aligned}zw&=(\cos\theta+\mathrm{i}\sin\theta)(\cos\psi+\mathrm{i}\sin\psi)\\&=(\cos\theta\cos\psi-\sin\theta\sin\psi)+\mathrm{i}(\sin\theta\cos\psi+\cos\theta\sin\psi).\end{aligned}$$

三角和公式表明

$$zw=\cos(\theta+\psi)+\mathrm{i}\sin(\theta+\psi).$$

加法定理给出了复数乘法的几何解释. ■

系 1.31 设 z 和 w 是极坐标分别为 (r,θ) 和 (s,ψ) 的复数，则 zw 的极坐标是[⊖]

$$(rs,\theta+\psi),$$

从而

$$|zw|=|z||w|.$$

证明 如果 z 和 w 的极式分解分别为 $z=r(\cos\theta+\mathrm{i}\sin\theta)$ 和 $w=s(\cos\psi+\mathrm{i}\sin\psi)$，则

$$zw=rs[\cos(\theta+\psi)+\mathrm{i}\sin(\theta+\psi)].$$ ■

15 ~ 16

特别地，如果 $|z|=1=|w|$，则 $|zw|=1$；即单位圆上两复数的积也在单位圆上.

⊖ 若 $\theta+\psi\leqslant 2\pi$，该公式是正确的；否则，这个角度应该是 $\theta+\psi-2\pi$.

1707年，棣莫弗（A. De Moiver，1667—1754）证明了下面的优美结果.

定理 1.32（棣莫弗） 对每个实数 x 和每个正整数 n，

$$\cos(nx)+i\sin(nx)=(\cos x+i\sin x)^n.$$

证明 对 $n\geqslant1$ 用归纳法证明棣莫弗定理. 基础步 $n=1$ 显然为真. 关于归纳步，

$$\begin{aligned}(\cos x+i\sin x)^{n+1}&=(\cos x+i\sin x)^n(\cos x+i\sin x)\\&=(\cos(nx)+i\sin(nx))(\cos x+i\sin x)\quad\text{（归纳假设）}\\&=\cos(nx+x)+i\sin(nx+x)\quad\text{（加法公式）}\\&=\cos([n+1]x)+i\sin([n+1]x).\end{aligned}$$

■

系 1.33

(ⅰ) $\cos(2x)=\cos^2x-\sin^2x=2\cos^2x-1$

$\sin(2x)=2\sin x\cos x.$

(ⅱ) $\cos(3x)=\cos^3x-3\cos x\sin^2x=4\cos^3x-3\cos x$

$\sin(3x)=3\cos^2x\sin x-\sin^3x=3\sin x-4\sin^3x.$

证明 (ⅰ)

$$\begin{aligned}\cos(2x)+i\sin(2x)&=(\cos x+i\sin x)^2\\&=\cos^2x+2i\sin x\cos x+i^2\sin^2x\\&=\cos^2x-\sin^2x+i(2\sin x\cos x).\end{aligned}$$

实部和实部相等，虚部和虚部相等给出两个倍角公式.

(ⅱ) 棣莫弗定理给出

$$\begin{aligned}\cos(3x)+i\sin(3x)&=(\cos x+i\sin x)^3\\&=\cos^3x+3i\cos^2x\sin x+3i^2\cos x\sin^2x+i^3\sin^3x\\&=\cos^3x-3\cos x\sin^2x+i(3\cos^2x\sin x-\sin^3x).\end{aligned}$$

实部相等得 $\cos(3x)=\cos^3x-3\cos x\sin^2x$;用 $1-\cos^2x$ 替换 $\sin^2x$ 得到 $\cos(3x)$ 的第二个公式. 虚部相等给出 $\sin(3x)=3\cos^2x\sin x-\sin^3x=3\sin x-4\sin^3x$，其中第二个公式是用 $1-\sin^2x$ 替换 $\cos^2x$ 而得到. ■

17

系 1.33 可以推广. 如果 $f_2(x)=2x^2-1$，则

$$\cos(2x)=2\cos^2x-1=f_2(\cos x),$$

如果 $f_3(x)=4x^3-3x$，则

$$\cos(3x)=4\cos^3x-3\cos x=f_3(\cos x).$$

命题 1.34 对于一切 $n\geqslant1$，存在整系数多项式 $f_n(x)$ 使得

$$\cos(nx)=f_n(\cos x).$$

证明 由棣莫弗定理，

$$\begin{aligned}\cos(nx)+i\sin(nx)&=(\cos x+i\sin x)^n\\&=\sum_{r=0}^{n}\binom{n}{r}\cos^{n-r}x\ i^r\sin^rx.\end{aligned}$$

左边的实部 $\cos(nx)$ 必等于右边的实部. 现在 i^r 是实数当且仅当 r 是偶数，因此

$$\cos(nx)=\sum_{r\text{为偶数}}\binom{n}{r}\cos^{n-r}x\ i^r\sin^rx.$$

如果 $r=2k$，则 $i^r=i^{2k}=(-1)^k$，从而

$$\cos(nx) = \sum_{k=0}^{\left[\frac{n}{2}\right]} (-1)^k \binom{n}{2k} \cos^{n-2k} x \sin^{2k} x,$$

其中$\left[\frac{n}{2}\right]$是$\leqslant \frac{n}{2}$的最大整数. 而 $\sin^{2k} x = (\sin^2 x)^k = (1-\cos^2 x)^k$ 是 $\cos x$ 的多项式，定理得证.

■

对 $n \geqslant 2$ 用归纳法，容易证明 $f_n(x)$ 的首项是 $2^{n-1}x^n$. 命题 1.34 的正弦版本可在习题 1.49 中找到.

欧拉 (Euler) 定理 对一切实数 x,

$$e^{ix} = \cos x + i \sin x.$$

撇开收敛性，证明的基本思想是考察 e^{ix}的幂级数展开式的实部和虚部. 用 i 的幂以长度 4 循环的事实：$1, i, -1, -i, 1, \cdots$，有

$$\begin{aligned} e^{ix} &= 1 + ix + \frac{(ix)^2}{2!} + \frac{(ix)^3}{3!} + \cdots \\ &= \left[1 - \frac{x^2}{2!} + \frac{x^4}{4!} + \cdots\right] + i\left[x - \frac{x^3}{3!} + \frac{x^5}{5!} + \cdots\right] \\ &= \cos x + i \sin x. \end{aligned}$$

18

据说欧拉特别喜欢等式

$$e^{\pi i} = -1;$$

这个公式甚至刻在了他的墓碑上.

作为欧拉定理的推论，极式分解可以重写为指数形式：每个复数 z 有因数分解

$$z = re^{i\theta},$$

其中 $r \geqslant 0, 0 \leqslant \theta < 2\pi$. 加法定理和棣莫弗定理也可以重新用复指数形式来表述. 加法定理成为

$$e^{ix}e^{iy} = e^{i(x+y)};$$

棣莫弗定理成为

$$(e^{ix})^n = e^{inx}.$$

定义 设 $n \geqslant 1$ 是整数，称满足 $\zeta^n = 1$ 的复数 ζ 为 **n 次单位根**.

当 z 和 w 在单位圆上时，即 $|z| = 1 = |w|$，复数乘法的几何解释特别有意思. 给定正整数 n，令 $\theta = 2\pi/n, \zeta = e^{i\theta}$. ζ 的极坐标是 $(1, \theta)$，ζ^2 的极坐标是$(1, 2\theta)$，ζ^3 的极坐标是$(1, 3\theta)$，…，ζ^{n-1}的极坐标是$(1, (n-1)\theta)$，$\zeta^n = 1$ 的极坐标是$(1, n\theta) = (1, 0)$. 于是 n 次单位根均匀地分布在单位圆上. 图 1.5 展示了 8 次单位根(这里 $\theta = 2\pi/8 = \pi/4$).

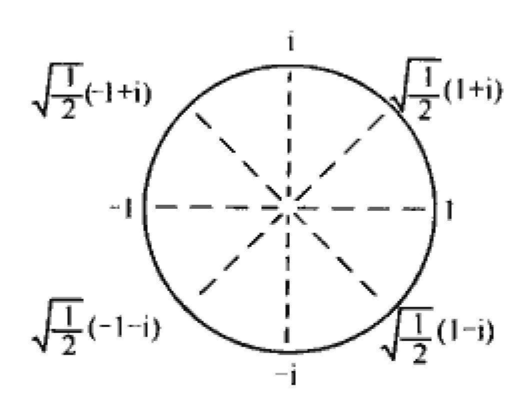


图 1.5 8 次单位根

19

系 1.35 每个 n 次单位根等于

$$e^{2\pi ik/n} = \cos\left(\frac{2\pi k}{n}\right) + i \sin\left(\frac{2\pi k}{n}\right),$$

其中 k 是 $0, 1, 2, \cdots, n-1$ 之中的某个数，因此它的模为 1.

证明 注意 $e^{2\pi i} = \cos 2\pi + i \sin 2\pi = 1$. 据棣莫弗定理，如果 $\zeta = e^{2\pi i/n} = \cos(2\pi/n) + i \sin(2\pi/n)$，则

$$\zeta^n = (e^{2\pi i/n})^n = e^{2\pi i} = 1,$$

从而 ζ 是 n 次单位根. 因 $\zeta^n=1$，从而对所有 $k=0,1,2,\cdots,n-1$，$(\zeta^k)^n=(\zeta^n)^k=1^k=1$，因此 $\zeta^k=e^{2\pi ik/n}$ 也是 n 次单位根. 我们已经列举了 n 个不同的 n 次单位根，在第3章中将证明 n 次有理系数多项式（例如 x^n-1）最多有 n 个复根，从而再没有其他的 n 次单位根. ■

正如数 a 有两个平方根，即 $\sqrt{a}$ 和 $-\sqrt{a}$，a 有 n 个不同的 n 次根，即 $e^{2\pi ik/n}\sqrt[n]{a}$，其中 $k=0,1,\cdots,n-1$.

每个 n 次单位根当然是多项式 x^n-1 的根. 所以

$$x^n-1=\prod_{\zeta^n=1}(x-\zeta).$$

如果 ζ 是一个 n 次单位根，而 n 是最小的正整数使得 $\zeta^n=1$，我们就称 ζ 为 **n 次单位原根**. 由此，i 是8次单位根，但不是8次单位原根，然而 i 是4次单位原根.

引理 1.36 *如果 n 次单位根 ζ 是 d 次单位原根，则 d 必是 n 的因数.*

证明 带余除法给出 $n=qd+r$，其中 q，r 是整数，余数 r 满足 $0\leqslant r<d$. 因为 $\zeta^{qd}=(\zeta^d)^q=1$，因此

$$1=\zeta^n=\zeta^{qd+r}=\zeta^{qd}\zeta^r=\zeta^r.$$

如果 $r\neq 0$，这便与 d 是最小的指数使得 $\zeta^d=1$ 相矛盾. 因此正如所断言的那样 $n=qd$. ■

定义 设 d 是正整数. 定义 d 阶**分圆多项式**[⊖]为

$$\Phi_d(x)=\prod(x-\zeta),$$

其中 ζ 遍历所有 d 次单位原根.

20

下面的结果几乎是显而易见的.

命题 1.37 *对每个整数 $n\geqslant 1$，*

$$x^n-1=\prod_{d|n}\Phi_d(x),$$

其中 d 遍历 n 的所有因数 d [特别地，$\Phi_1(x)$ 和 $\Phi_n(x)$ 出现在其中].

证明 依据系1.35，该命题不过是对 n 的每个因数 d 把等式 $x^n-1=\prod(x-\zeta)$ 中 ζ 为 d 次单位原根的项归并在一起. ■

例如，如果 p 是素数，则 $x^p-1=\Phi_1(x)\Phi_p(x)$. 因为 $\Phi_1(x)=x-1$，于是有

$$\Phi_p(x)=x^{p-1}+x^{p-2}+\cdots+x+1.$$

定义 定义**欧拉 ϕ-函数**为 n 阶分圆多项式的次数：

$$\phi(n)=\deg(\Phi_n(x)).$$

现在给出欧拉 ϕ-函数的另一种不依赖于单位根的描述.

命题 1.38 *对每个 $n\geqslant 1$，有*

$$n=\sum_{d|n}\phi(d).$$

证明 注意 $\phi(n)$ 是 $\Phi_n(x)$ 的次数，并用如下事实：多项式乘积的次数是各因式次数的和. ■

命题 1.39 *设 $n\geqslant 1$ 是整数，则 $\phi(n)$ 是满足 $1\leqslant k\leqslant n$ 且 $(k,n)=1$ 的整数 k 的个数.*

⊖ x^n-1 的根是 n 次单位根：$1,\zeta,\zeta^2,\cdots,\zeta^{n-1}$，其中 $\zeta=e^{2\pi i/n}=\cos(2\pi/n)+i\sin(2\pi/n)$. 现在这些根把单位圆 $\{z\in\mathbb{C}:|z|=1\}$ 分成 n 段等弧（见图1.5）. 这就解释了术语 cyclotomic（分圆），因为它的希腊原意是 circle splitting（分圆）.

证明 只需证明 $e^{2\pi ik/n}$是 n 次单位原根当且仅当 k 和 n 互素.

如果 k 和 n 不互素，则 $n=dr$，$k=ds$，其中 d，r，s 是整数且 $d>1$. 由此 $r<n$ 且 $\frac{k}{n}=\frac{ds}{dr}=\frac{s}{r}$，于是 $(e^{2\pi ik/n})^r=(e^{2\pi is/r})^r=1$，所以 $e^{2\pi ik/n}$不是 n 次单位原根.

反之，假设 $\zeta=e^{2\pi ik/n}$不是 n 次单位原根，引理 1.36 说 ζ 必是 n 的某个因数 d 的 d 次单位根，其中 $d<n$，即存在 $1\leqslant m\leqslant d$ 使得

$$\zeta=e^{2\pi ik/n}=e^{2\pi im/d}=e^{2\pi imr/dr}=e^{2\pi imr/n}.$$

因 k 和 mr 都排在 1 和 n 之间，从而 $k=mr$（如果 $0\leqslant x$，$y\leqslant 1$，且 $e^{2\pi ix}=e^{2\pi iy}$，则 $x=y$），即 r 是 k 和 n 的因数，从而 k 和 n 不互素. ■

回忆多项式 $f(x)$ 的**首项系数**是指出现在 $f(x)$ 中的 x 的最高幂的系数. 如果一个多项式的首项系数为 1，则称该多项式为**首一**多项式.

[21]

命题 1.40 对每个正整数 n，分圆多项式 $\Phi_n(x)$ 是整系数首一多项式.

证明 对 $n\geqslant 1$ 用归纳法证明. 因 $\Phi_1(x)=x-1$，基础步成立. 关于归纳步，假设 $\Phi_d(x)$ 是整系数首一多项式，从等式 $x^n-1=\prod_d \Phi_d(x)$，有

$$x^n-1=\Phi_n(x)f(x),$$

其中 $f(x)$ 是一切 $\Phi_d(x)$ 的积，$d<n$ 且 d 是 n 的因数. 由归纳假设，$f(x)$ 是整系数首一多项式. 因为 $f(x)$ 是首一多项式，长除法（即多项式的带余除法）表明 $\Phi_n(x)=(x^n-1)/f(x)$ 的所有系数正如所要的都是整数[⊖]. ■

下面的系将用来证明第 8 章中的韦德伯恩（Wedderburn）定理.

系 1.41 设 q 是正整数，d 是整数 n 的因数且 $d<n$，则 $\Phi_n(q)$ 既是 q^n-1 的因数也是 $(q^n-1)/(q^d-1)$ 的因数.

证明 我们已经知道 $x^n-1=\Phi_n(x)f(x)$，其中 $f(x)$ 是整系数首一多项式. 令 $x=q$ 得整数等式 $q^n-1=\Phi_n(q)f(q)$，即 $\Phi_n(q)$ 是 q^n-1 的因数.

如果 d 是 n 的因数且 $d<n$，考虑等式 $x^d-1=\prod(x-\zeta)$，其中 ζ 遍历 d 次单位根. 注意，因为 d 是 n 的因数，因此每个这样的 ζ 是一个 n 次单位根. 又因 $d<n$，组合等式 $x^n-1=\prod(x-\zeta)$ 中的项得

$$x^n-1=\Phi_n(x)(x^d-1)g(x),$$

其中 $g(x)$ 是这样一些分圆多项式 $\Phi_\delta(x)$ 的积：δ 是 n 的因数，$\delta<n$，且 δ 不是 d 的因数. 从上一命题知，$g(x)$ 是整系数首一多项式. 所以 $g(q)\in\mathbb{Z}$，从而

$$\frac{x^n-1}{x^d-1}=\Phi_n(x)g(x)$$

给出结论. ■

求复数的倒数有一个简单的方法. 如果 $z=a+ib\in\mathbb{C}$，其中 a，$b\in\mathbb{R}$，定义它的**复共轭**为 $\bar{z}=a-ib$. 注意 $z\bar{z}=a^2+b^2=|z|^2$，从而 $z\neq 0$ 当且仅当 $z\bar{z}\neq 0$. 如果 $z\neq 0$，则

$$z^{-1}=1/z=\bar{z}/z\bar{z}=(a/z\bar{z})-i(b/z\bar{z});$$

即

⊖ 如果不清楚，参见带余除法的证明.

[22]

$$\frac{1}{a+\mathrm{i}b}=\left(\frac{a}{a^2+b^2}\right)-\mathrm{i}\left(\frac{b}{a^2+b^2}\right).$$

如果 $|z|=1$，则 $z^{-1}=\bar{z}$. 特别是，如果 z 是单位根，则它的倒数就是它的复共轭.

复共轭满足下列恒等式：

$$\overline{z+w}=\bar{z}+\bar{w};$$
$$\overline{zw}=\bar{z}\,\bar{w};$$
$$\bar{\bar{z}}=z;$$
$$\bar{z}=z \quad \text{当且仅当 } z \text{ 是实数.}$$

我们已经把复数看成平面上的点，和向量演算一样，点 z 等同于从原点 O 到 z 的箭头所表示的向量$\overrightarrow{Oz}$. 定义 $z=a+\mathrm{i}b$ 和 $w=c+\mathrm{i}d$ 的**点积**为

$$z\cdot w=ac+bd.$$

于是，$z\cdot w=|z||w|\cos\theta$，其中 θ 是$\overrightarrow{Oz}$和$\overrightarrow{Ow}$之间的夹角［因 $\cos\theta=\cos(2\pi-\theta)$，无论 θ 是$\overrightarrow{Oz}$到$\overrightarrow{Ow}$的夹角，还是$\overrightarrow{Ow}$到$\overrightarrow{Oz}$的夹角，结果都一样］. 注意

$$z\cdot z=|z|^2=z\bar{z}.$$

显然 $z\cdot w=w\cdot z$，且容易验证对所有复数 z，w 和 w'，

$$z\cdot(w+w')=z\cdot w+z\cdot w'$$

下面的结果将用来证明第 8 章中的伯恩赛德（Burnside）定理.

命题 1.42 设 ε_1，…，ε_n 是单位根，其中 $n\geqslant 2$，则

$$\left|\sum_{j=1}^{n}\varepsilon_j\right|\leqslant\sum_{j=1}^{n}|\varepsilon_j|=n.$$

此外，等号成立当且仅当一切 ε_j 都相等.

证明 不等式的证明对 $n\geqslant 2$ 用归纳法. 基础步得自**三角不等式**：对一切复数 u 和 v，

$$|u+v|\leqslant|u|+|v|.$$

归纳步的证明很简单，因为单位根的模为 1.

现在假设一切 ε_j 都相等，比如对一切 j，$\varepsilon_j=\varepsilon$，则显然有等式 $\left|\sum_{j=1}^{n}\varepsilon_j\right|=|n\varepsilon|=n|\varepsilon|=n$. 逆命题的证明是对 $n\geqslant 2$ 用归纳法. 关于基础步，假设 $|\varepsilon_1+\varepsilon_2|=2$. 运用点积有

$$\begin{aligned}4&=|\varepsilon_1+\varepsilon_2|^2\\&=(\varepsilon_1+\varepsilon_2)\cdot(\varepsilon_1+\varepsilon_2)\\&=|\varepsilon_1|^2+2\varepsilon_1\cdot\varepsilon_2+|\varepsilon_2|^2\\&=2+2\varepsilon_1\cdot\varepsilon_2.\end{aligned}$$

[23]

因此，$2=1+\varepsilon_1\cdot\varepsilon_2$，于是

$$\begin{aligned}1&=\varepsilon_1\cdot\varepsilon_2\\&=|\varepsilon_1||\varepsilon_2|\cos\theta\\&=\cos\theta,\end{aligned}$$

其中 θ 是$\overrightarrow{O\varepsilon_1}$和$\overrightarrow{O\varepsilon_2}$之间的夹角（因为 $|\varepsilon_1|=1=|\varepsilon_2|$）. 所以 $\theta=0$ 或 $\theta=\pi$，由此 $\varepsilon_2=\pm\varepsilon_1$. 因为 $\varepsilon_2=-\varepsilon_1$ 给出 $|\varepsilon_2+\varepsilon_1|=0$，所以必有 $\varepsilon_2=\varepsilon_1$.

关于归纳步，假设 $\left|\sum_{j=1}^{n+1}\varepsilon_j\right|=n+1$. 如果 $\left|\sum_{j=1}^{n}\varepsilon_j\right|<n$，则三角不等式给出

$$\left|\left(\sum_{j=1}^{n}\varepsilon_j\right)+\varepsilon_{n+1}\right|\leqslant\left|\sum_{j=1}^{n}\varepsilon_j\right|+1<n+1,$$

这与假设矛盾. 所以 $\left|\sum_{j=1}^{n}\varepsilon_j\right|=n$，由归纳假设，$\varepsilon_1$，…，$\varepsilon_n$ 都相等，比如等于 ω，因此 $\sum_{j=1}^{n}\varepsilon_j=n\omega$，从而

$$|n\omega+\varepsilon_{n+1}|=n+1.$$

与基础步的推导一样：

$$\begin{aligned}(n+1)^2&=(n\omega+\varepsilon_{n+1})\cdot(n\omega+\varepsilon_{n+1})\\&=n^2+2n\omega\cdot\varepsilon_{n+1}+1,\end{aligned}$$

于是 $1=\omega\cdot\varepsilon_{n+1}=|\omega||\varepsilon_{n+1}|\cos\theta$，其中 θ 是 $\overrightarrow{O\omega}$ 和 $\overrightarrow{O\varepsilon_{n+1}}$ 之间的夹角. 因此 $\omega=\pm\varepsilon_{n+1}$，且进一步有 $\omega=\varepsilon_{n+1}$. ■

习题

1.43 计算 $(\cos3°+i\sin3°)^{40}$.

1.44 (i) 求 $(3+4i)/(2-i)$.

(ii) 设 $z=re^{i\theta}$，证明 $z^{-1}=r^{-1}e^{-i\theta}$.

(iii) 求 $\sqrt{i}$ 的值.

(iv) 证明 $e^{i\theta/n}$ 是 $e^{i\theta}$ 的 n 次根.

1.45 求 $\Phi_6(x)$.

1.46 如果 α 是满足 $\cos(\pi\alpha)=\frac{1}{3}$ 的数（其中角度 $\pi\alpha$ 是弧度），证明 α 是无理数.

提示：如果 $\alpha=\frac{m}{n}$，用棣莫弗定理计算 $\cos(n\pi\alpha)+i\sin(n\pi\alpha)$.

1.47 设 $f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$ 是实系数多项式. 证明：如果 z 是 $f(x)$ 的根，则 $\bar{z}$ 也是 $f(x)$ 的根.

24

1.48 (i) 证明二次多项式的求根公式对复系数二次多项式也成立.

(ii) 求 $x^2+(2+i)x+2i$ 的根. 为什么两根复共轭?

1.49 证明对每个奇整数 $n\geqslant1$，存在整系数多项式 $g_n(x)$ 满足

$$\sin nx=g_n(\sin x).$$

1.50 每个毕达哥拉斯三元组 (a,b,c) 确定一个直角边为 a 和 b 斜边[⊖]为 c 的直角三角形. 称两个毕达哥拉斯三元组 (a,b,c) 和 (a',b',c') 相似，如果它们确定的直角三角形是相似三角形，即对应边成比例.

(i) 证明对毕达哥拉斯三元组 (a,b,c) 和 (a',b',c') 的下述陈述等价.

(1) (a,b,c) 和 (a',b',c') 相似.

(2) 存在正整数 m 和 ℓ 使得 $(ma,mb,mc)=(\ell a',\ell b',\ell c')$.

(3) $\frac{a}{c}+i\frac{b}{c}=\frac{a'}{c'}+i\frac{b'}{c'}$.

(ii) 证明每个毕达哥拉斯三元组与一个本原毕达哥拉斯三元组相似.

1.51 (i) 如果一个模 1 的复数的实部和虚部都是有理数，则称该复数为有理的. 如果 $\frac{a}{c}+i\frac{b}{c}$ 是 a，b 都不

⊖ Hypotenuse（斜边）来自意为“to stretch（张紧）”的希腊字.

为零的有理复数，证明（$|a|$，$|b|$，$|c|$）是毕达哥拉斯三元组.

（ⅱ）证明两个有理复数的积也是有理复数，并用此事实定义两个毕达哥拉斯三元组的积（不计相似）.（3,4,5）和它自己的积是什么？

（ⅲ）证明毕达哥拉斯三元组 (a,b,c) 的平方是 $(a^2-b^2, 2ab, a^2+b^2)$.

1.3 集合论

和数学的一切领域一样，函数在代数中也随处可见，现讨论这一概念.

集合 X 是一些元素（数、点、鲱鱼等）的集族. 用

$$x \in X$$

记 x 属于 X. 如果两个集合 X 和 Y 由完全相同的元素组成，即 $x \in X$ 当且仅当 $x \in Y$，称两集合 X 和 Y **相等**，记作

$$X = Y,$$

集合 X 的**子集**是指这样的集合 S，它的每个元素都属于集合 X：如果 $s \in S$ 则 $s \in X$. 记 S 是 X 的子集为

25

$$S \subseteq X;$$

同义词是"X **包含** S"和"S **包含于** X". 注意，恒有 $X \subseteq X$. 如果 $S \subseteq X$ 且 $S \neq X$，则称 S 是 X 的**真子集**，记为 $S \subsetneq X$. 由定义可知，两集合 X 和 Y 相等当且仅当它们互为子集，即

$$X = Y \quad \text{当且仅当} \quad X \subseteq Y \text{ 且 } Y \subseteq X.$$

基于这一注释，证明两集合相等往往分作两步，每一步证明一个集合是另一个的子集. 例如，设

$$X = \{a \in \mathbb{R} : a \geqslant 0\} \quad \text{和} \quad Y = \{r^2 : r \in \mathbb{R}\}.$$

如果 $a \in X$，则 $a \geqslant 0$，从而 $a = r^2$，其中 $r = \sqrt{a}$. 因此 $a \in Y$ 从而 $X \subseteq Y$. 关于反包含，取 $r^2 \in Y$. 如果 $r \geqslant 0$，则 $r^2 \geqslant 0$；如果 $r < 0$，则 $r = -s$，其中 $s > 0$. 于是 $r^2 = (-1)^2 s^2 = s^2 \geqslant 0$. 两种情形都有 $r^2 \geqslant 0$，从而 $r^2 \in X$. 于是 $Y \subseteq X$，从而 $X = Y$.

微积分书中定义函数为一个"法则"，对每个数 a，按照这一法则确定唯一的数（记作 $f(a)$）与之对应. 当然，这一定义其精神可嘉，但有缺陷：法则是什么？或者用另一种问法，何时两法则相同？例如，考虑函数

$$f(x) = (x+1)^2 \quad \text{和} \quad g(x) = x^2 + 2x + 1.$$

$f(x) = g(x)$ 吗？它们的计算方法当然是不同的：例如，$f(6) = (6+1)^2 = 7^2$，而 $g(6) = 6^2 + 2 \cdot 6 + 1 = 36 + 12 + 1$. 因为术语*法则*是不加定义的，有歧义的，因而这个问题没有答案. 如果不能确定两个函数是否相同，那么微积分描述的定义实在是不充分的.

函数的图像是具体的事物［例如，$f(x) = x^2$ 的图像是抛物线］，将要给出的函数的正式定义相当于说函数就是它的图像. 微积分把函数当作法则的非正式定义是残缺的，我们要避开法则是什么的问题. 为了给出定义，先要有一个类似于平面的东西［因为我们要求函数 $f(x)$ 的自变量不总是数］.

定义 *设 X 和 Y 是两个集合（可以相等），它们的***笛卡儿积** *$X \times Y$ 是一切有序对 (x, y) 的集合，其中 $x \in X$，$y \in Y$.*

平面是 $\mathbb{R} \times \mathbb{R}$.

关于有序对唯一需要知道的是

$$(x,y)=(x',y') \quad \text{当且仅当} \quad x=x' \text{和} y=y'$$

(见习题 1.62).

如果 X 和 Y 是有限集，比如 $|X|=m$ 和 $|Y|=n$（记有限集 X 中元素的个数为 $|X|$），则 $|X\times Y|=mn$.

26

定义 设 X 和 Y 是两个集合（可以相等）. 如果子集 $f\subseteq X\times Y$ 满足对每个 $a\in X$，有唯一的 $b\in Y$ 使得 $(a,b)\in f$，则称 f 为 X 到 Y **函数**，记为[⊖]

$$f: X\to Y.$$

对每一个 $a\in X$，满足 $(a,b)\in f$ 的唯一元素 $b\in Y$ 称为 f 在 a 处的**值**，且记 b 为 $f(a)$. 于是，f 由 $X\times Y$ 中一切形如 $(a,f(a))$ 的点组成. 当 $f:\mathbb{R}\to\mathbb{R}$ 时，f 是 $f(x)$ 的图像.

称 X 为 f 的**定义域**，称 Y 为 f 的**目标域**（或上域），定义由 f 的一切值组成的 Y 的子集为 f 的**象**（或值域），记为 $\mathrm{im} f$.

定义 设 $f: X\to Y$ 和 $g: X'\to Y'$ 是两个函数，如果 $X=X'$，$Y=Y'$ 且子集 $f\subseteq X\times Y$ 和子集 $g\subseteq X'\times Y'$ 也相等，则称这两个函数**相等**.

例如，X 是集合，则**恒等函数** $1_X: X\to X$ 定义为对一切 $x\in X$，$1_X(x)=x$. 如果 $X=\mathbb{R}$，则 $1_{\mathbb{R}}$ 是过原点斜率为 1 的直线. 如果 $f: X\to Y$ 是函数，S 是 X 的子集，则 f 在 S 上的**限制**是指函数 $f|S: S\to X$，其定义为对一切 $s\in S$，$(f|S)(s)=f(s)$. 如果 S 是集合 X 的子集，**包含**是指函数 $i: S\to X$，其定义为对一切 $s\in S$，$i(s)=s$. 如果 S 是 X 的真子集，则包含 i 不是恒等函数 1_S，因为它的目标域是 X 而不是 S，i 也不是恒等函数 1_X，因为它的定义域是 S 而不是 X.

函数 $f: X\to Y$ 有三个要素：定义域、目标域和象. 两函数相等当且仅当它们有相同的定义域、相同的目标域和相同的象.

很清楚，定义域和象是函数的核心要素. 既然函数的象更重要，为什么还要关注它的目标域呢?

在实际情形中，起初定义函数时，往往不知道它的象. 例如，实值函数 $f:\mathbb{R}\to\mathbb{R}$ 由 $f(x)=x^2+3x-8$ 给出后，我们才能分析 f 求它的象. 但如果目标域必须是象，则不先求出 f 的象就无法写下 $f: X\to Y$（求出精确的象即便不是不可能，也常常是十分困难的），于是，使用目标域是方便的.

在线性代数中考虑向量空间 V 和它的对偶空间 $V^*=\{V\text{ 上的一切线性泛函}\}$（也是向量空间）. 此外，每个线性变换 $T: V\to W$ 定义了一个线性变换

$$T^*: W^*\to V^*,$$

且 T^* 的定义域 W^* 由 T 的目标域 W 所确定.（事实上，如果关于 T 的矩阵是 A，则关于 T^* 的矩阵是 A^t，它是 A 的转置矩阵.）于是，改变 T 的目标域就改变了 T^* 的定义域，因此，T^* 的改变是在 T 的目标域不可缺少的方式下进行的.

27

命题 1.43 设 $f: X\to Y$ 和 $g: X\to Y$ 是函数，则 $f=g$ 当且仅当对每个 $a\in X$，$f(a)=g(a)$.

注 该命题解决了由有歧义的术语法则引起的问题. 如果 $f,g:\mathbb{R}\to\mathbb{R}$ 由 $f(x)=(x+1)^2$ 和 $g(x)=x^2+2x+1$ 给出，因为对每个数 a，$f(a)=g(a)$，故 $f=g$.

⊖ 从现在起，记函数为 f 以替代 $f(x)$，记号 $f(x)$ 只表示 f 在 x 处的值，但有少数例外，如继续使用 $\sin x$，e^x 和 x^2 等.

证明 假设 $f=g$. 函数是 $X\times Y$ 的子集；所以 $f=g$ 说明 f 和 g 互为子集（非正式地说，f 和 g 有相同的图像）. 如果 $a\in X$，则 $(a,f(a))\in f=g$，于是 $(a,f(a))\in g$. 但 g 中只有一个以 a 为第一坐标的有序对，即 $(a,g(a))$（因为函数的定义说 g 在 a 处的值唯一）. 所以 $(a,f(a))=(a,g(a))$，从该有序对的相等得到所要的 $f(a)=g(a)$.

反之，假设对每个 $a\in X, f(a)=g(a)$. 要证 $f=g$ 只需证明 $f\subseteq g$ 且 $g\subseteq f$. f 的每个元素形为 $(a,f(a))$. 由 $f(a)=g(a)$ 得 $(a,f(a))=(a,g(a))$，从而 $(a,f(a))\in g$. 所以 $f\subseteq g$. 同样可证反过来的包含关系 $g\subseteq f$. ■

可以继续把函数 f 看作将 $x\in X$ 射到 $y\in Y$ 的法则，但在必要时可使用精确定义，如命题 1.43 的证明. 然而，在重新把函数 $f: X\to Y$ 看作一种动力机构把 X 中的点射到 Y 中的点的时候，常用

$$f: x\mapsto y$$

代替 $f(x)=y$. 例如，可用 $x\mapsto x^2$ 来代替 $f(x)=x^2$，以及对一切 x 用 $x\mapsto x$ 来描述恒等函数.

常说函数 f 是**合理定义的**（或单值的）而不说 f 的值是唯一的. 公式 $g(a/b)=ab$ 定义了一个函数 $g:\mathbb{Q}\to\mathbb{Q}$ 吗？分数的写法有很多种. 因为 $\frac{1}{2}=\frac{3}{6}$，可知 $g\left(\frac{1}{2}\right)=1\cdot 2\neq 3\cdot 6=g\left(\frac{3}{6}\right)$，从而 g 不是合理定义的，所以 g 不是函数. 要是公式 $g(a/b)=ab$ 只对 a/b 是既约形式时成立，则 g 是函数.

公式 $f(a/b)=3a/b$ 定义了一个函数 $f:\mathbb{Q}\to\mathbb{Q}$，因为它是合理定义的：如果 $a/b=a'/b'$，可以证明

$$f(a/b)=3a/b=3a'/b'=f(a'/b').$$

由 $a/b=a'/b'$ 得 $ab'=a'b$，由此 $3ab'=3a'b$ 且 $3a/b=3a'/b'$. 从而 f 确实是一个函数，即 f 是合理定义的.

例 1.44 我们的定义可以处理一种退化的情形. 如果 X 是集合，什么是函数 $X\to\varnothing$？首先注意 $X\times\varnothing$ 的元素是有序对 (x,y)，其中 $x\in X$，$y\in\varnothing$. 因为没有 $y\in\varnothing$，所以没有这样的有序对，从而 $X\times\varnothing=\varnothing$. 函数 $X\to\varnothing$ 是 $X\times\varnothing$ 的某个子集，但 $X\times\varnothing=\varnothing$，这样只有一个子集就是 $\varnothing$，由此最多有一个函数即 $f=\varnothing$. 函数 $X\to\varnothing$ 的定义说，对每个 $x\in X$，存在唯一的 $y\in\varnothing$ 满足 $(x,y)\in f$. 如果 $X\neq\varnothing$，则存在 $x\in X$，对于它不存在这样的 y（$\varnothing$ 中根本没有任何元素 y），所以 f 不是函数. 于是，如果 $X\neq\varnothing$，则没有函数从 X 到 $\varnothing$. 另一方面，如果 $X=\varnothing$，则 $f=\varnothing$ 是函数. 否则"f 是函数"的否命题为"存在 $x\in\varnothing$，等等". 不必再继续说下去，因为没有元素在 $\varnothing$ 中，这个句子无法完成，因此原命题为真. 总之，$f=\varnothing$ 是函数 $\varnothing\to\varnothing$，称它为恒等函数 $1_{\varnothing}$. ■

28

函数的象为整个目标域的特殊情形有一个名称.

定义 称函数 $f: X\to Y$ 是**满射**(或上的) 如果

$$\operatorname{im} f=Y.$$

这样，如果对每个 $y\in Y$，存在某个 $x\in X$（可能依赖于 y）使得 $y=f(x)$，则 f 是满射.

下面的定义给出函数可能具有的另一个重要性质.

定义 设 $f: X\to Y$ 是函数，如果对于 X 的不同元素 a 和 a' 必有 $f(a)\neq f(a')$，则称该函数是**单射**(或一一的). 等价地（逆否命题），称 f 是单射，如果关于每对 a，$a'\in X$ 有

$$f(a)=f(a') \text{ 蕴涵 } a=a'.$$

读者要注意单射是合理定义的倒置：如果 $a=a'$ 蕴涵 $f(a)=f(a')$，则 f 是合理定义的；如果 $f(a)=f(a')$ 蕴涵 $a=a'$，则 f 是单射.

这些函数还有别的名称. 满射常称为**满态射**，单射常称为**单态射**. 记号 $A\twoheadrightarrow B$ 表示满射，记号

$A \hookrightarrow B$ 或 $A \rightarrowtail B$ 表示单射. 但本书不用这些术语和记号.

例 1.45 考虑由 $f(x)=3x-4$ 给出的函数 $f:\mathbb{R}\to\mathbb{R}$. 要知道 f 是否是满射，取 $y\in\mathbb{R}$ 并问是否存在 $a\in\mathbb{R}$ 使得 $y=3a-4$. 解得 $a=\frac{1}{3}(y+4)$，由此可断言 f 是满射. 如果 $3a-4=3b-4$，则 $a=b$，所以 f 也是单射，

作为第二个例子，考虑由

$$g(x)=\frac{3x-4}{x-1}$$

给出的函数 $g:\mathbb{R}-\{1\}\to\mathbb{R}$.

29

如果 $(3a-4)/(a-1)=(3b-4)/(b-1)$，则交错相乘得 $a=b$，所以 g 是单射. 另一方面，g 不是满射，给定 $y\in\mathbb{R}$，是否有 $a\in\mathbb{R}$ 使得 $y=(3a-4)/(a-1)$？解得 $a=(4-y)/(3-y)$，此式提示 $y=3$ 不是 g 的值，它确实不是 g 的值，因为 $3=(3a-4)/(a-1)$ 无解. ■

定义 设 $f:X\to Y$ 和 $g:Y\to Z$ 是函数（注意 f 的目标域等于 g 的定义域），则它们的**复合**记为 $g\circ f$，是指由

$$g\circ f: x\mapsto g(f(x))$$

给出的函数 $X\to Z$. 即先求 f 在 x 上的值，再求 g 在 $f(x)$ 上的值.

微积分中的链式法则是用 g' 和 f' 表出导数 $(g\circ f)'$ 的公式：

$$(g\circ f)'=[g'\circ f]\cdot f'.$$

例如

$$(\sin(\ln x))'=\cos(\ln x)\cdot\frac{1}{x}.$$

给定集合 X，令

$$\mathcal{F}(X)=\{X\to X\ 的一切函数\}.$$

刚才已经知道 $\mathcal{F}(X)$ 中两个函数的复合总是有定义的，且复合后也是 $\mathcal{F}(X)$ 中的函数. 于是可以看作在 $\mathcal{F}(X)$ 上配置了一种乘法，该乘法不满足**交换律**，即 $f\circ g$ 和 $g\circ f$ 未必相等. 例如，设 $f(x)=x+1$，$g(x)=x^2$，则 $f\circ g: 1\mapsto 1^2+1=2$ 而 $g\circ f: 1\mapsto(1+1)^2=4$，所以，$f\circ g\neq g\circ f$.

引理 1.46

(i) 复合满足结合律：如果

$$f:X\to Y, g:Y\to Z\ 和\ h:Z\to W$$

是函数，则

$$h\circ(g\circ f)=(h\circ g)\circ f.$$

(ii) 如果 $f:X\to Y$，则 $1_Y\circ f=f=f\circ 1_X$.

证明概要 用命题 1.43. ■

$\mathcal{F}(X)$ 中有没有“倒数”，即对于任一函数 f，存在 $g\in\mathcal{F}(x)$ 使得 $f\circ g=1_X$ 和 $g\circ f=1_X$ 吗？

定义 称函数 $f:X\to Y$ 为**双射**（或一一对应）如果它既是单射又是满射.

30

定义 称函数 $f:X\to Y$ 有**逆**如果存在函数 $g:Y\to X$ 使得 $g\circ f$ 和 $f\circ g$ 两者都是恒等函数.

命题 1.47 (i) 如果 $f:X\to Y$ 和 $g:Y\to X$ 是函数满足 $g\circ f=1_X$，则 f 是单射，g 是满射.

(ii) 函数 $f:X\to Y$ 有逆 $g:Y\to X$ 当且仅当 f 是双射.

证明 (i) 假设 $f(x)=f(x')$，运用 g 得 $g(f(x))=g(f(x'))$；即 $x=x'$ [因为 $g(f(x))=$

$x]$，因此 f 是单射.如果 $x \in X$，则 $x = g(f(x))$，由此 $x \in \operatorname{im} g$，所以 g 是满射.

（ii）如果 f 有逆 g，则因为 $g \circ f$ 和 $f \circ g$ 两者都是恒等函数，由（i）知 f 既是单射又是满射.

假定 f 是双射.对每个 $y \in Y$，因 f 是满射，所以有 $a \in X$ 使得 $f(a) = y$，因为 f 是单射，所以这个 a 是唯一的. 定义 $g(y) = a$，这就给出了一个定义域为 Y 的（合理定义的）函数，易知 g 是 f 的逆，即对一切 $y \in Y$，$f(g(y)) = f(a) = y$ 和对一切 $a \in X$，$g(f(x)) = g(y) = a$. ■

注 习题 1.59 证明如果 f 和 g 两者都是单射，则它们的复合 $f \circ g$ 也是单射. 同样，如果 f 和 g 两者都是满射则它们的复合 $f \circ g$ 也是满射. 由此，两个双射的复合也是双射.

记号 记双射 f 的逆为 f^{-1}（习题 1.54 说一个函数不能有两个逆）.

例 1.48 这个例子给出两个函数 f 和 g 的一种复合 $g \circ f$ 是恒等函数，而另一种复合 $f \circ g$ 不是恒等函数，于是，f 和 g 不是互逆函数.

设 $N = \{n \in \mathbb{Z} : n \geqslant 0\}$，定义 $f, g : \mathbb{N} \to \mathbb{N}$ 如下：

$$f(n) = n + 1;$$

$$g(n) = \begin{cases} 0 & \text{当 } n = 0 \\ n-1 & \text{当 } n \geqslant 1. \end{cases}$$

因 $n+1 \geqslant 1$，所以 $g(f(n)) = g(n+1) = n$，所以复合函数 $g \circ f = 1_{\mathrm{N}}$. 另一方面，因 $f(g(0)) = f(0) = 1 \neq 0$，所以 $f \circ g \neq 1_{\mathrm{N}}$.

31

注意 f 是单射但不是满射，g 是满射但不是单射. ■

有两种方案可用来判定所给函数是否是双射：(1) 用单射和满射的定义；(2) 求逆. 例如，记正实数为 $\mathbb{R}^{>}$，证明由 $f(x) = \mathrm{e}^x = \sum x^n/n!$ 定义的指数函数 $f : \mathbb{R} \to \mathbb{R}^{>}$ 是双射. 最简单的是用（自然）对数 $g(y) = \ln y = \int_1^y \mathrm{d}t/t$. 常用公式 $\mathrm{e}^{\ln y} = y$ 和 $\ln \mathrm{e}^x = x$ 表明 $f \circ g$ 和 $g \circ f$ 两个复合都是恒等函数，从而 f 和 g 是互逆函数. 因 f 有逆，f 是双射.（直接证明 f 是单射需要证明：若 $\mathrm{e}^a = \mathrm{e}^b$，则 $a = b$；直接证明 f 是满射要牵涉到证明如下的事实：对每个正实数 c，都有某个 a 使它可以表示为 e^a 的形式.）

总结刚才得到的结果.

定理 1.49 记集合 X 到其自身的全体双射的集合为 S_X. 函数的复合有下列性质：

（i）如果 $f, g \in S_X$，则 $f \circ g \in S_X$；

（ii）对一切 $f, g, h \in S_X$，$h \circ (g \circ f) = (h \circ g) \circ f$；

（iii）恒等函数 1_X 在 S_X 中，且对每个 $f \in S_X$，$1_X \circ f = f = f \circ 1_X$；

（iv）对每个 $f \in S_X$，存在 $g \in S_X$ 使得 $g \circ f = 1_X = f \circ g$.

证明概要（i）由习题 1.59 得到，该题证明两个双射的复合也是双射. 其他部分上面已经证明. ■

设 X 和 Y 是集合，函数 $f : X \to Y$ 定义了一种"前移作用"，把 X 的子集移作 Y 的子集，也就是说，如果 $S \subseteq X$，则

$$f(S) = \{y \in Y : \text{有某个 } s \in S \text{ 使得 } y = f(s)\},$$

它还定义了一种"后退作用"，把 Y 的子集移作 X 的子集，也就是说，如果 $W \subseteq Y$，则

$$f^{-1}(W) = \{x \in X : f(x) \in W\}.$$

称 $f^{-1}(W)$ 为 W 的**原象**. 正式陈述：记集合 X 全体子集的族为 $\mathcal{P}(X)$，如果 $f: X \to Y$，则由 $f_*: S \mapsto f(S)$ 给出函数

$$f_*: \mathcal{P}(X) \to \mathcal{P}(Y),$$

由 $f^*: W \mapsto f^{-1}(W)$ 给出函数

$$f^*: \mathcal{P}(Y) \to \mathcal{P}(X).$$

当 f 是满射时，这些作用在 Y 的全体子集和 X 的某些子集间建立了一个双射.

32

命题 1.50 设 X 和 Y 是集合，并设 $f: X \to Y$ 是满射.

(i) 如果 $T \subseteq S$ 是 X 的子集，则 $f(T) \subseteq f(S)$；如果 $U \subseteq V$ 是 Y 的子集，则 $f^{-1}(U) \subseteq f^{-1}(V)$.

(ii) 如果 $U \subseteq Y$，则 $ff^{-1}(U) = U$.

(iii) 复合函数 $f_* f^*: \mathcal{P}(Y) \to \mathcal{P}(Y) = 1_{\mathcal{P}(Y)}$，由此 $f^*: W \mapsto f^{-1}(W)$ 是单射.

(iv) 如果 $S \subseteq X$，则 $S \subseteq f^{-1}f(S)$，但可能有严格的包含关系.

注 如果 f 不是满射，则 $W \mapsto f^{-1}(W)$ 未必是单射：比如有 $y \in Y$ 而 $y \notin f(X)$，则 $f^{-1}(\{y\}) = \varnothing = f^{-1}(\varnothing)$.

证明 (i) 如果 $y \in f(T)$，则有某个 $t \in T$ 使得 $y = f(t)$. 但是 $t \in S$，这是因为 $T \subseteq S$，从而 $f(t) \in f(S)$，所以 $f(T) \subseteq f(S)$. 容易证明另一个包含关系.

(ii) 如果 $u \in U$，则 f 是满射表明有 $x \in X$ 使得 $f(x) = u$，因此 $x \in f^{-1}(U)$，从而 $u = f(x) \in ff^{-1}(U)$. 至于反包含，设 $a \in ff^{-1}(U)$，则有某个 $x' \in f^{-1}(U)$ 使得 $a = f(x')$，这就证明了所要的 $a = f(x') \in U$.

(iii) (ii) 说明 $f_* f^* = 1_{\mathcal{P}(Y)}$，由命题 1.47，$f^*$ 是单射.

(iv) 如果 $s \in S$，则 $f(s) \in f(S)$，由此 $s \in f^{-1}f(s) \subseteq f^{-1}f(S)$.

为证明可能存在严格的包含关系，设 $f: \mathbb{R} \to \mathbb{C}$ 由 $x \mapsto e^{2\pi i x}$ 给出，如果 $S = \{0\}$，则 $f(S) = \{1\}$，而 $f^{-1}f(\{1\}) = \mathbb{Z}$. ■

在习题 1.68 中可以看到，如果 $f: X \to Y$，则原象在子集上的表现比象更好. 例如，对 $S, T \subseteq Y$, $f^{-1}(S \cap T) = f^{-1}(S) \cap f^{-1}(T)$，但对于 $A, B \subseteq X$，有可能 $f(A \cap B) \neq f(A) \cap f(B)$.

需要用到多于两个集合的笛卡儿积. 可以把元素 $(x_1, x_2) \in X_1 \times X_2$ 看作函数 $f: \{1,2\} \to X_1 \cup X_2$，其中对 $i = 1,2, f(i) = x_i \in X_i$.

定义 设 I 是集合，$\{X_i, i \in I\}$ 是加标的集合族. 称集合

$$\prod_{i \in I} X_i = \{f: I \to \bigcup_{i \in I} X_i : \text{对一切 } i \in I, f(i) \in X_i\}$$

为**笛卡儿积**.

可以把元素 $x \in \prod_i X_i$ 看作"向量" $x = (x_i)$，对 $i \in I$，该"向量"的第 i 个坐标为 $x_i = f(i)$. 如果 I 是有限的，比如 $I = \{1, 2, \cdots, n\}$，则不难理解 $\prod_i X_i = X_1 \times \cdots \times X_n$，其中右端的集合是由

$$X_1 \times \cdots \times X_{n+1} = (X_1 \times \cdots \times X_n) \times X_{n+1}$$

归纳定义的. 如果指标集 I 是无限的且一切 X_i 都非空，则 $\prod_{i \in I} X_i$ 非空并不是明显的. 的确，这一论断与选择公理等价（见附录）.

需要比函数概念更广泛的关系的概念.

33

定义 设 X 和 Y 是集合. 称子集 $R \subseteq X \times Y$ 为 **X 到 Y 的关系**. 常用

$$x\,R\,y$$

记 $(x,y)\in R$. 如果 $X=Y$，则称 R 为 X **上的关系**.

为使读者确信这一定义是合情合理的，这里给出一个具体的解释. 通常认为$\leqslant$是$\mathbb{R}$上的关系，其实它就是关系定义的体现. 设

$$R=\{(x,y)\in\mathbb{R}\times\mathbb{R}:(x,y)\text{ 在直线 }y=x\text{ 上或在它的上方}\}.$$

读者会看出 $x\,R\,y$ 当且仅当有通常意义下的 $x\leqslant y$ 时成立.

例 1.51 (i) 函数 $f:X\to Y$ 是关系.

(ii) 任一集合 X 上的相等是关系，它是对角线

$$\Delta_X=\{(x,x)\in X\times X\}.$$

(iii) 在任一集合上空集$\varnothing$定义了一个关系，但它没有什么意思. ■

定义 称集合 X 上的关系 $x\equiv y$ 是

自反的：如果对一切 $x\in X, x\equiv x$；

对称的：如果对一切 $x,y\in X, x\equiv y$ 蕴涵 $y\equiv x$；

传递的：如果对一切 $x,y,z\in X, x\equiv y$ 且 $y\equiv z$ 蕴涵 $x\equiv z$.

有以上三性质（自反、对称、传递）的关系称为**等价关系**.

例 1.52 (i) 集合 X 上的相等是等价关系，可把等价关系看作一种广义相等.

(ii) 对任一整数 $m\geqslant 0$，mod$m$ 的同余是$\mathbb{Z}$上的等价关系. ■

集合 X 上的等价关系生成 X 的一个子集族.

定义 设$\equiv$是集合 X 上的等价关系. 对 $a\in X$，a 的**等价类**记为 $[a]$，定义为

$$[a]=\{x\in X:x\equiv a\}\subseteq X.$$

例如，在 mod$m$ 的同余下，整数 a 的等价类 $[a]$ 称为 a 的**同余类**.

34 下一引理说明，把元素替换成它们的等价类之后，等价就变成真正的相等.

引理 1.53 设$\equiv$是集合 X 上的等价关系，则 $x\equiv y$ 当且仅当 $[x]=[y]$.

证明 假定 $x\equiv y$. 如果 $z\in[x]$，则 $z\equiv x$，由传递性得 $z\equiv y$，因此 $[x]\subseteq[y]$. 由对称性，$y\equiv x$，于是得反包含 $[y]\subseteq[x]$. 因此 $[x]=[y]$.

反之，如果 $[x]=[y]$，则由自反性，$x\in[x]$，从而 $x\in[x]=[y]$，因此 $x\equiv y$. ■

定义 称集合 X 的子集 A_i 的族**两两不交**，如果对一切 $i\neq j$，

$$A_i\cap A_j=\varnothing.$$

如果两两不交的非空子集族的并是整个 X，则称该子集族为集合 X 的**划分**，称这些子集为块.

命题 1.54 设$\equiv$是集合 X 上的等价关系，则等价类形成 X 的划分. 反之，给出 X 的一个划分 $\{A_i:i\in I\}$，就有一个以块 A_i 为等价类的 X 上的等价关系.

证明 假定给定了 X 上的等价关系$\equiv$，因$\equiv$是自反的，所以每个 $x\in X$ 在等价类 $[x]$ 中，由此等价类是非空子集，其并是 X. 为证两两不交，假定 $a\in[x]\cap[y]$，于是 $a\equiv x$ 且 $a\equiv y$. 由对称性，$x\equiv a$，再由传递性，$x\equiv y$. 据引理有 $[x]=[y]$，所以等价类形成 X 的划分.

反之，设 $\{A_i:i\in I\}$ 是 X 的划分. 对 $x,y\in X$，定义 $x\equiv y$，如果存在 $i\in I$ 使得 $x\in A_i, y\in A_i$. 十分清楚，$\equiv$是自反的和对称的. 为证明$\equiv$的传递性，假定 $x\equiv y, y\equiv z$，即存在 $i,j\in I$ 使得 $x,y\in A_i, y,z\in A_j$. 因 $y\in A_i\cap A_j$. 由两两不交得 $A_i=A_j$，从而 $i=j$ 且 $x,z\in A_i$，即 $x\equiv z$. 以上证明了$\equiv$是等价关系.

剩下的要证明等价类是各个 A_i. 如果 $x\in X$，则有某个 i 使得 $x\in A_i$. 由 $\equiv$ 的定义，如果 $y\in A_i$，则 $y\equiv x$ 且 $y\in[x]$，因此 $A_i\subseteq[x]$. 关于反包含，设 $z\in[x]$，于是 $z\equiv x$，即有某个 j 使得 $x\in A_j, z\in A_j$，因此 $x\in A_i\cap A_j$；由两两不交得 $i=j$，由此 $z\in A_i$ 且 $[x]\subseteq A_i$. 所以 $[x]=A_i$. ■

例 1.55 （ⅰ）刚才已经知道由划分可以定义集合上的等价关系. 设 $I=[0,1]$ 是单位闭区间，定义 I 的划分如下：一个块是两点集 $\{0,1\}$，其他是一点集 $\{a\}$，其中 $0<a<1$. 全体块的族，即全体等价类的族可以当作一个圆，因为区间的两个端点看作是等同的.

35

用 $\mathbb{R}$ 代替 I，得到圆的另一种构造. 定义 $\mathbb{R}$ 上的关系 $a\equiv b$ 如果 $a-b\in\mathbb{Z}$，容易看出这是 $\mathbb{R}$ 上的等价关系，数 a 的等价类是

$$[a]=\{r\in\mathbb{R}: r=a+n, n\in\mathbb{Z}\}\}$$

全体块的族仍然是圆（长为 1 的任一区间的端点看作是等同的）.

（ⅱ）在正方形 $I\times I$ 上定义等价关系如下：对于每个 $a\in I$，$\{(a,0),(a,1)\}$ 是一个块，对每个 $b\in I$，$\{(0,b),(1,b)\}$ 是一个块，其他是正方形内部的单点集 $\{(a,b)\}$. 全体等价类的族可以当成一个**圆环**（油炸圈饼的表面）：把正方形的左右两边粘合得到圆柱面，再粘合圆柱面的顶端和底端得到圆环. ■

习题

1.52 设 X 和 Y 是集合，$f: X\to Y$ 是函数. 如果 S 是 X 的子集，证明限制 $f\mid S$ 等同于复合 $f\circ i$，其中 $i: S\to X$ 是包含映射.

提示：用命题 1.43.

1.53 如果 $f: X\to Y$ 有逆 g，证明 g 是双射.

提示：g 有逆吗？

1.54 证明：如果 $f: X\to Y$ 是双射，则它恰有一个逆.

1.55 证明由 $f(x)=3x+5$ 定义的 $f:\mathbb{R}\to\mathbb{R}$ 是双射，并求它的逆.

1.56 判定由

$$f(a/b,c/d)=(a+c)/(b+d)$$

定义的 $f:\mathbb{Q}\times\mathbb{Q}\to\mathbb{Q}$ 是函数.

1.57 设 $X=\{x_1,\cdots x_m\}$ 和 $Y=\{y_1,\cdots,y_n\}$ 是有限集. 证明存在双射 $f: X\to Y$ 当且仅当 $|X|=|Y|$，即 $m=n$.

提示：如果 f 是双射，则在 Y 中有 m 个不同的元素 $f(x_1),\cdots,f(x_m)$，因此 $m\leqslant n$；f 换成 f^{-1} 可得反过来的不等式 $n\leqslant m$.

1.58 如果 X 和 Y 是元素个数相同的有限集，证明对于函数 $f: X\to Y$，下列条件等价：

（ⅰ）f 是单射.

（ⅱ）f 是双射.

（ⅲ）f 是满射.

提示：如果 $A\subseteq X$ 且 $|A|=n=|X|$，究竟 X 中还有多少元素不在 A 中？

1.59 设 $f: X\to Y$ 和 $g: Y\to Z$ 是函数.

（ⅰ）如果 f 和 g 两者都是单射，则 $g\circ f$ 也是单射.

（ⅱ）如果 f 和 g 两者都是满射，则 $g\circ f$ 也是满射.

（ⅲ）如果 f 和 g 两者都是双射，则 $g\circ f$ 也是双射.

36

（iv）如果 $g\circ f$ 是双射，证明 f 是单射，g 是满射.

1.60 设 $f:(-\pi/2,\pi/2)\to\mathbb{R}$ 由 $a\mapsto\tan a$ 定义，证明 f 有逆函数 g，它就是 $g=\arctan$.

1.61 如果 A 和 B 都是集合 X 的子集，定义

$$A-B=\{a\in A:a\notin B\}.$$

证明 $A-B=A\cap B'$，其中 $B'=X-B$ 是 B 的补集，即

$$B'=\{x\in X:x\notin B\}.$$

1.62 设 A 和 B 是集合，且设 $a\in A,b\in B$. 定义它们的**有序对**如下：

$$(a,b)=\{a,\{a,b\}\}.$$

如果 $a'\in A,b'\in B$，证明 $(a',b')=(a,b)$ 当且仅当 $a'=a,b'=b$.

提示：制约 $\in$ 关系的公理之一是命题

$$a\in x\in a$$

恒假.

1.63 （i）为证明集合 X 上对称的、传递的关系 R 是自反的，下面的论证错在哪里？如果 $x\in X$，则取 $y\in X$ 满足 xRy，由对称性得 yRx，由传递性得 xRx.

（ii）举出集合上关系的例子，要求它是对称的、传递的，但不是自反的.

1.64 （i）设 X 是集合，且 $R\subseteq X\times X$，定义 $\widetilde{R}=\bigcap_{R'\in\mathcal{E}}R'$，其中 $\mathcal{E}$ 是 X 上一切包含 R 的等价关系 R' 组成的族. 证明 $\widetilde{R}$ 是 X 上的等价关系（称 $\widetilde{R}$ 为 R **生成的等价关系**）.

（ii）设 R 是集合 X 上自反、对称的关系，证明 R 生成的等价关系 $\widetilde{R}$ 由所有这样的 $(x,y)\in X\times X$ 所组成：存在有限多个 $(x,y)\in R$，比如 $(x_1,y_1),\cdots,(x_n,y_n)$，使得 $x=x_1,y_n=y$，且对一切 $i\geqslant 1,y_i=x_{i+1}$.

1.65 设 $X=\{(a,b):a,b\in\mathbb{Z}$，且 $b\neq 0\}$，定义 X 上的关系 $(a,b)\equiv(c,d)$，如果 $ad=bc$. 证明它是 X 上的等价关系.（1，2）的等价类是什么？

1.66 定义 $\mathbb{C}$ 上的关系 $z\equiv w$，如果 $|z|=|w|$. 证明它是 $\mathbb{C}$ 上的等价关系，它的等价类是原点和以原点为圆心的圆.

1.67 （i）设 $f:X\to Y$ 是函数（其中 X 和 Y 是集合），定义 X 上的关系 $x\equiv x'$，如果 $f(x)=f(x')$. 证明它是等价关系.

（ii）定义 $f:\mathbb{R}\to S^1$ 为 $f(x)=e^{2\pi ix}$，其中 $S^1\subseteq\mathbb{C}$ 是单位圆，在（i）中的等价关系下，0 的等价类是什么？

1.68 设 $f:X\to Y$ 是函数，设 $V,W\subseteq Y$.

（i）证明

37

$$f^{-1}(V\cap W)=f^{-1}(V)\cap f^{-1}(W)\text{ 和 }f^{-1}(V\cup W)=f^{-1}(V)\cup f^{-1}(W).$$

（ii）证明 $f(V\cup W)=f(V)\cup f(W)$.

（iii）举例说明 $f(V\cap W)\neq f(V)\cap f(W)$.

（iv）证明 $f^{-1}(W')=(f^{-1}(W))'$，其中 $W'=\{y\in Y:y\notin W\}$ 是 W 的补集. 举出函数 f 的例子，使其满足对某个 $S\subseteq X$ 有 $f(S')\neq(f(S))'$.

38

第2章 群 I

2.1 引言

自 16 世纪发现了解三次和四次多项式的求根公式之后，延续约 300 年未解决的一个大问题是寻找次数更高的多项式的求根公式. 起先 100 年间，数学家们考虑数到底是什么，因为三次公式迫使人们产生负数是否是数，和复数是否也是数的合法存在形式这样的问题. 到 1800 年，鲁菲尼(P. Ruffini)宣称不存在五次多项式的求根公式（与二次、三次、四次形式相同的公式；即只用算术运算和 n 次根表示的公式），但他的同时代人没有接受他的证明（他的想法其实是正确的，但他的证明有漏洞）. 1815 年，柯西(A. L. Cauchy)引入了置换的乘法并证明了我们称之为对称群 S_n 的基本性质，例如他引入了轮换的记号并证明了置换可唯一地分解为不相交的轮换. 1824 年，阿贝尔(N. Abel,1802—1829)给出一个可以接受的五次公式不存在的证明，在他的证明中，用 1770 年拉格朗日(J. L. Lagrange)引入的某种有理函数构造了五次根的置换. 伽罗瓦(E. Galois,1811—1832)这位在 21 岁生日前被杀的青年奇才，修改了有理函数，而更重要的是他看到了解开问题的关键是包含其中的他称之为*群*的概念：S_n 在乘法下封闭的子集——用我们今天的话说，就是 S_n 的*子群*. 他把每个多项式 $f(x)$ 和一个群联系起来，今日称之为 $f(x)$ 的*伽罗瓦群*. 他认识了共轭、正规子群、商群和单群，并证明（用我们的语言）一个多项式（在特征 0 的域上）有像二次公式那样的求根公式，当且仅当它的伽罗瓦群是*可解群*（可解性是交换性的推广）. 这是一个绝好的事例，足以说明伽罗瓦是近世代数最重要的奠基人之一. 有关这个问题的历史的精辟论述，我们推荐 J. P. Tignol 的著作《Galois Theory of Algebraic Equations》.

39

本章除了提到在第一门课程中通常不讲授的材料之外，也要复习一些熟知的结果，对于这些结果的证明只有概要.

2.2 置换

在伽罗瓦看来，群是由某些置换（多项式的根的置换）组成的，今日置换的群仍有其重要性.

定义 *集合 X 的置换是 X 到其自身的双射.*

在高中数学中，把集合 X 的置换定义为它的元素的一次重排. 例如 $X=\{1,2,3\}$ 有六种重排方式：

$$123;\quad 132;\quad 213;\quad 231;\quad 312;\quad 321.$$

现在设 $X=\{1,2,\cdots,n\}$ 一次重排是 X 的所有元素的一张表，其中无重复元素，对于这种表我们所能做的就是计算它们的个数，n 个元素的集合 X 恰有 $n!$ 个置换.

现在 X 的一次重排 $i_1,i_2,\cdots,i_n$ 确定了一个函数 $\alpha: X\to X$，即 $\alpha(1)=i_1,\alpha(2)=i_2,\cdots,\alpha(n)=i_n$. 例如重排为 213，它确定的函数 α 是 $\alpha(1)=2,\alpha(2)=1,\alpha(3)=3$. 我们用排成两行的记号来表示重排对应的函数：如果 $\alpha(j)$ 是表中的第 j 项，则

$$\alpha=\begin{pmatrix}1 & 2 & \cdots & j & \cdots & n\\ \alpha(1) & \alpha(2) & \cdots & \alpha(j) & \cdots & \alpha(n)\end{pmatrix}.$$

表包含 X 的所有元素说明对应的函数 α 是满射，底下一行是 $\operatorname{im}\alpha$. 表中无重复元素说明不同的点有不同的值；即 α 是单射. 于是每张表确定一个双射 $\alpha: X \to X$；即每次重排确定一个置换. 反之，每个置换 α 确定一次重排，就是底下一行列出的 $\alpha(1), \alpha(2), \cdots, \alpha(n)$. 所以重排和置换只不过是同一事物的不同描述方法，然而，把置换看作函数的好处是可以对它们进行复合，习题 1.59 表明置换的复合仍是置换.

定义 称集合 X 的全体置换的族为 X 上的**对称群**，记为 S_X. 当 $X = \{1,2,\cdots,n\}$ 时，常用 S_n 来记 S_X，并称之为 **n 个字母上的对称群**.

为简化记号，用 $\beta\alpha$ 代替 $\beta \circ \alpha$，用 (1) 代替 1_X.

注意 S_3 中的复合是不交换的. 置换排成两行的记号除了麻烦之外，还有一个主要问题，就是它遮盖了一些基本问题的答案，比如，两置换可交换吗？一个置换的平方是恒等函数吗？下面引入的特殊置换将弥补这个缺陷.

40

定义 设 $i_1, i_2, \cdots, i_r$ 是 $\{1,2,\cdots,n\}$ 中的不同整数. 如果 $\alpha \in S_n$ 固定其他整数（如果有的话），且

$$\alpha(i_1) = i_2, \alpha(i_2) = i_3, \cdots, \alpha(i_{r-1}) = i_r, \alpha(i_r) = i_1,$$

则称 α 为一个 **r-轮换**，也称 α 为**长 r** 的轮换，记为

$$\alpha = (i_1 i_2 \cdots i_r).$$

2-轮换把 i_1 和 i_2 对调而固定其余的不动，2-轮换也称为**对换**. 1-轮换是恒等函数，因为它固定每个 i. 由此一切 1-轮换都相等：对一切 i，$(i) = (1)$.

术语轮换（cycle）来自意为圆的希腊字. 轮换 $(i_1\ i_2\ \cdots\ i_r)$ 可如图 2.1 所示画为圆上的顺时针旋转.

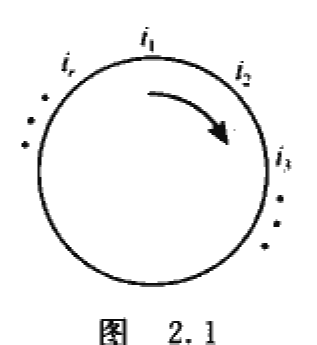


图 2.1

任一 i_j 可作为“起点”，由此任一 r-轮换有 r 种不同的轮换记号：

$$(i_1 i_2 \cdots i_r) = (i_2 i_3 \cdots i_r i_1) = \cdots = (i_r i_1 i_2 \cdots i_{r-1}).$$

现在给出把置换分解成轮换乘积的一种算法. 例如取

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 7 & 2 & 5 & 1 & 8 & 9 & 3 \end{pmatrix}.$$

一开始写下“(1”. 因 $\alpha: 1 \mapsto 6$，所以写“(1 6”. 其次，因 $\alpha: 6 \mapsto 1$，所以括号关闭：α 变成“(1 6)”. 未出现的第一个数字是 2，由此接着写“(1 6)(2”. 因 $\alpha: 2 \mapsto 4$，所以写“(1 6)(2 4”. 因 $\alpha: 4 \mapsto 2$，括号再次关闭，并写“(1 6)(2 4)”. 剩下的最小数字是 3，由 $3 \mapsto 7$，$7 \mapsto 8$，$8 \mapsto 9$ 和 $9 \mapsto 3$ 得 4-轮换 (3 7 8 9). 最后 $\alpha(5) = 5$. 可以断言

41

$$\alpha = (1\ 6)(2\ 4)(3\ 7\ 8\ 9)(5).$$

因为 S_n 中的乘积是函数的复合，所以上面的断言是说对于 1 到 9 之间的每个 i，

$$\alpha(i) = [(1\ 6)(2\ 4)(3\ 7\ 8\ 9)(5)](i)$$

[毕竟两个函数 f 和 g 相等当且仅当对于它们定义域中的每个 i 有 $f(i) = g(i)$]. 右端是复合 $\beta\gamma\delta$ 的

值，其中 $\beta=(1\ 6),\gamma=(2\ 4),\delta=(3\ 7\ 8\ 9)$ [1-轮换(5)可忽略不计，因为它是恒等函数]. 现在 $\alpha(1)=6$，再计算右端 $i=1$ 时复合函数的值.

$$\begin{aligned}\beta\gamma\delta(1)&=\beta(\gamma(\delta(1)))\\&=\beta(\gamma(1)) &&\delta=(3\ 7\ 8\ 9)\text{ 固定 }1\\&=\beta(1) &&\gamma=(2\ 4)\text{ 固定 }1\\&=6 &&\beta=(1\ 6).\end{aligned}$$

类似地，对每个 i，有 $\alpha(i)=\beta\gamma\delta(i)$，这就证明了上面的断言.

因为置换的乘积是函数的复合，所以置换的乘法自右到左；即要求 $\alpha\beta(1)$，我们计算 $\alpha(\beta(1))$. 另一个例子是计算 S_5 中的乘积

$$\sigma=(1\ 2)(1\ 3\ 4\ 2\ 5)(2\ 5\ 1\ 3).$$

为了求出 σ 的排成两行的记号，从轮换的右端开始计算：

$$\begin{aligned}&\sigma: 1\mapsto 3\mapsto 4\mapsto 4;\\&\sigma: 2\mapsto 5\mapsto 1\mapsto 2;\\&\sigma: 3\mapsto 2\mapsto 5\mapsto 5;\\&\sigma: 4\mapsto 4\mapsto 2\mapsto 1;\\&\sigma: 5\mapsto 1\mapsto 3\mapsto 3.\end{aligned}$$

于是[⊖]，

$$\sigma=\begin{pmatrix}1&2&3&4&5\\4&2&5&1&3\end{pmatrix}.$$

把前面的算法运用到 σ 的这个排成两行的记号上得

$$\sigma=(1\ 4)(2)(5\ 3).$$

在上面进行的把置换分解为轮换的算法中，我们注意到轮换族在下列意义下不相交. [42]

定义 称两个置换 $\alpha,\beta\in S_n$ **不相交**，如果每个 i 被一个移动而被另一个固定：如果 $\alpha(i)\neq i$，则 $\beta(i)=i$，且如果 $\beta(j)\neq j$，则 $\alpha(j)=j$. 称置换族 $\beta_1,\cdots,\beta_t$ **不相交**，如果它们两两不相交.

引理 2.1 不相交置换 $\alpha,\ \beta\in S_n$ 可交换.

证明 只需证明：如果 $1\leqslant i\leqslant n$，则 $\alpha\beta(i)=\beta\alpha(i)$. 如果 β 移动 i，比如，$\beta(i)=j\neq i$，则 β 也移动 j [否则，$\beta(j)=j,\beta(i)=j$，这与 β 是单射矛盾]. 因 α 和 β 不相交，$\alpha(i)=i,\alpha(j)=j$，因此 $\beta\alpha(i)=j=\alpha\beta(i)$. 如果 α 移动 i 可得同样结论. 最后，如果 α 和 β 都固定 i，显然 $\beta\alpha(i)=\alpha\beta(i)$. ■

命题 2.2 每个置换 $\alpha\in S_n$ 不是一个轮换就是不相交轮换的乘积.

证明 对由 α 移动的点数 k 用归纳法证明. 基础步 $k=0$ 为真，因为现在 α 是 1-轮换的恒等置换.

如果 $k>0$，设 i_1 是被 α 移动的点. 定义 $i_2=\alpha(i_1),i_3=\alpha(i_2),\cdots,i_{r+1}=\alpha(i_r)$，其中 r 是满足 $i_{r+1}\in\{i_1,i_2,\cdots,i_r\}$ 的最小整数(因为只有 n 个可能的值，所以表 $i_1,i_2,i_3,\cdots,i_k$，…最终必有重复). 我们断言 $\alpha(i_r)=i_1$. 否则，有某个 $j\geqslant 2$ 使得 $\alpha(i_r)=i_j$，而 $\alpha(i_{j-1})=j$ 与假设 α 是单射矛盾. 令 σ 为 r-轮换 $(i_1\ i_2\ i_3\cdots i_r)$. 如果 $r=n$，则 $\alpha=\sigma$. 如果 $r<n$，则 σ 固定 Y 中的每个点，其中 Y 由剩下的 $n-r$ 个点组成，而 $\alpha(Y)=Y$. 定义 α' 为如下的置换：对 $i\in Y$，

⊖ 有些作者的置换乘法与此不同，他们的 $\alpha\circ\beta$ 是我们的 $\beta\circ\alpha$. 这是由于他们把"函数放在右边"：我们写作 $\alpha(i)$，他们写作 $(i)\alpha$. 考虑置换 α 和 β 先用 β 再用 α 的复合. 我们写作 $i\mapsto\beta(i)\mapsto\alpha(\beta(i))$，右边的记号为 $i\mapsto(i)\beta\mapsto((i)\beta)\alpha$. 由此，记号的改变引起乘法次序的改变.

$\alpha'(i)=\alpha(i)$，而固定所有的 $i\notin Y$. 注意到

$$\alpha=\sigma\alpha'.$$

归纳假设给出 $\alpha'=\beta_1\cdots\beta_t$，其中 $\beta_1,\cdots,\beta_t$ 是不相交的轮换. 因 σ 和 α' 不相交，所以 $\alpha=\sigma\beta_1\cdots\beta_t$ 是不相交轮换的乘积. ■

通常我们不允许 1-轮换出现在因子分解中 [因为 1-轮换是恒等置换 (1)]. 然而，如果有被 α 固定的 i，则对每个被 α 固定的 i，令 α 的因子分解中出现一个 1-轮换，从而 1-轮换有可能出现好几次.

定义 置换 α 的**完全轮换分解**是指 α 分解为不相交轮换的轮换分解，其中对每个被 α 固定的 i 恰有一个 1-轮换 (i).

例如，S_5 中的 3-轮换 $(1\ 3\ 5)$ 的完全轮换分解是 $\alpha=(1\ 3\ 5)(2)(4)$.

r-轮换 $\beta=(i_1\ i_2\ \cdots\ i_r)$ 和它的幂 β^k 之间有一种关系，其中 β^k 表示 β 和它自己复合 k 次. 注意 $i_2=\beta(i_1), i_3=\beta(i_2)=\beta(\beta(i_1))=\beta^2(i_1), i_4=\beta(i_3)=\beta(\beta^2(i_1))=\beta^3(i_1)$，更一般地，对一切 $k<r$，

43

$$i_{k+1}=\beta^k(i_1).$$

定理 2.3 设 $\alpha\in S_n$，并设 $\alpha=\beta_1\cdots\beta_t$ 是分解为不相交轮换的完全轮换分解. 如果不计分解中轮换出现的次序，则该分解是唯一的.

证明概要 因为在 α 的每个完全轮换分解中，对每个被 α 固定的 i 恰有一个 1-轮换，所以只需考虑分解为长度$\geqslant 2$ 的不相交轮换(不是完全轮换分解). 令 $\alpha=\gamma_1\cdots\gamma_s$ 是第二个把 α 分解为不相交轮换的这种分解.

对 t 和 s 的大者ℓ用归纳法证明该定理. 归纳步的开始注意到，如果 β_t 移动 i_1，则对一切 $k\geqslant 1, \beta_t^k(i_1)=\alpha^k(i_1)$. 此时必有某个 γ_j 也移动 i_1，因为不相交轮换可交换，我们可假定 γ_s 移动 i_1. 由此 $\beta_t=\gamma_s$，右乘 β_t^{-1} 得 $\beta_1\cdots\beta_{r-1}=\gamma_1\cdots\gamma_{s-1}$. ■

每个置换都是双射，如何求它的逆? 在轮换 β 的图形表示中，β 是圆上的顺时针旋转，逆 β^{-1} 就是逆时针旋转. 下一命题的证明是简单的.

命题 2.4 (i) 轮换 $\alpha=(i_1\ i_2\ \cdots\ i_r)$ 的逆是轮换 $(i_r\ i_{r-1}\cdots i_1)$:

$$(i_1 i_2\cdots i_r)^{-1}=(i_r\ i_{r-1}\cdots i_1).$$

(ii) 如果 $\gamma\in S_n$，且 $\gamma=\beta_1\cdots\beta_k$，则

$$\gamma^{-1}=\beta_k^{-1}\cdots\beta_1^{-1}.$$

定义 称两个置换 $\alpha,\beta\in S_n$ 有**相同的轮换结构**，如果在它们的完全轮换分解中，对每个 r，它们所含的 r-轮换个数相等.

根据习题 2.4，S_n 中共有

$$(1/r)[n(n-1)\cdots(n-r+1)]$$

个 r-轮换，该公式可用来计算具有给定轮换结构的置换的个数，但要注意轮换分解中出现几个等长轮换的情形. 例如，S_4 中形如 $(ab)(cd)$ 的置换个数是 $\frac{1}{2}\left[\frac{1}{2}(4\times 3)\right]\times\left[\frac{1}{2}(2\times 1)\right]=3$，乘以"额外"的因数 $\frac{1}{2}$ 是为了不把 $(ab)(cd)=(cd)(ab)$ 算作两个.

例 2.5 (i) 表 2.1 列出了 $G=S_4$ 中各种类型的置换个数.

表 2.1 S_4 中的置换

轮换结构	个数
(1)	1
(1 2)	6
(1 2 3)	8
(1 2 3 4)	6
(1 2) (3 4)	3
	24

44

（ⅱ）表 2.2 列出了 $G=S_5$ 中各种类型的置换个数.

表 2.2 S_5 中的置换

轮换结构	个数
(1)	1
(1 2)	10
(1 2 3)	20
(1 2 3 4)	30
(1 2 3 4 5)	24
(1 2) (3 4 5)	20
(1 2) (3 4)	15
	120

■

有一个计算的辅助手段，在陈述一般结果之前，先用下面的例子加以说明.

例 2.6 设 $\gamma=(1\ 3)(2\ 4\ 7)(5)(6)$，$\alpha=(2\ 5\ 6)(1\ 4\ 3)$，则

$$\alpha\gamma\alpha^{-1}=(4\ 1)(5\ 3\ 7)(6)(2)=(\alpha 1\ \alpha 3)(\alpha 2\ \alpha 4\ \alpha 7)(\alpha 5)(\alpha 6).$$ ■

引理 2.7 如果 $\gamma,\alpha\in S_n$，则 $\alpha\gamma\alpha^{-1}$ 与 γ 有相同的轮换结构. 详细地说，如果 γ 的完全轮换分解是

$$\gamma=\beta_1\beta_2\cdots(i_1\,i_2\cdots)\cdots\beta_t,$$

则 $\alpha\gamma\alpha^{-1}$ 可以这样得到：在 γ 的轮换中把 α 作用到各个记号上.

证明 证明的思想是 $\gamma\alpha\gamma^{-1}:\gamma(i_1)\mapsto i_1\mapsto i_2\mapsto\gamma(i_2)$. 用 σ 记引理陈述中所定义的置换.

如果 γ 固定 i，则 σ 固定 $\alpha(i)$，因为 σ 的定义说 $\alpha(i)$ 位于 σ 的轮换分解中的一个 1-轮换中. 另一方面，因为 γ 固定 i，$\alpha\gamma\alpha^{-1}$ 也固定 $\alpha(i)$：

$$\alpha\gamma\alpha^{-1}(\alpha(i))=\alpha\gamma(i)=\alpha(i).$$

假定 γ 移动记号 i_1，比如 $\gamma(i_1)=i_2$，于是 γ 的完全轮换分解中的一个轮换是

$$(i_1\ i_2\cdots).$$

由 σ 的定义，它的一个轮换是

$$(k\ell\cdots),$$

其中 $\alpha(i_1)=k$，$\alpha(i_2)=\ell$，因此 $\sigma:k\mapsto\ell$. 但 $\alpha\gamma\alpha^{-1}:k\mapsto i_1\mapsto i_2\mapsto\ell$，于是 $\alpha\gamma\alpha^{-1}(k)=\sigma(k)$. 所以 σ 和 $\alpha\gamma\alpha^{-1}$ 在一切形如 $k=\alpha(i_1)$ 的符号上是一致的. 因为 α 是满射，所以每个 k 都是这种形式，从而 $\sigma=$

$\alpha\gamma\alpha^{-1}$. ■

[45] **例 2.8** 在本例中说明引理 2.7 的逆命题也成立，其一般性证明由下一个定理给出．在 S_5 中，把 3-轮换 β 的完全轮换分解放在 3-轮换 γ 的上面，定义 α 为下移函数．例如，如果

$$\beta = (1\ 2\ 3)(4)(5)$$
$$\gamma = (5\ 2\ 4)(1)(3),$$

则

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 4 & 1 & 3 \end{pmatrix},$$

由此，$\alpha = (1\ 5\ 3\ 4)$．现在 $\alpha \in S_5$，且

$$\gamma = (\alpha 1\ \alpha 2\ \alpha 3),$$

由引理 2.7，$\gamma = \alpha\beta\alpha^{-1}$．注意，改写 β 的轮换，如 $\beta = (1\ 2\ 3)(5)(4)$，则给出 α 的另一种选取法． ■

定理 2.9 *S_n 中置换 γ 和 σ 有相同的轮换结构当且仅当存在 $\alpha \in S_n$ 使得 $\sigma = \alpha\gamma\alpha^{-1}$.*

证明概要 充分性已在引理 2.7 中得到证明．关于必要性，把一个完全轮换分解放在另一个的上面，使得下面的每一个轮换都在上面的一个等长轮换之下：

$$\gamma = \delta_1\delta_2\cdots(i_1 i_2\cdots)\cdots\delta_t$$
$$\sigma = \eta_1\ \eta_2\cdots(k\ell\cdots)\cdots\ \eta_t.$$

和例子中一样定义 α 为"下移"函数，因此 $\alpha(i_1) = k, \alpha(i_2) = \ell$，等等．因为 γ 的轮换分解中没有重复的符号(诸轮换 η 不相交)，所以 α 是置换，根据引理可知 $\sigma = \alpha\gamma\alpha^{-1}$． ■

置换还有一种有用的因子分解.

命题 2.10 *如果 $n \geqslant 2$，则每个 $\alpha \in S_n$ 都是对换的乘积.*

证明概要 根据命题 2.2，只需把 r-轮换 β 分解为对换的乘积．这一分解可以如下进行：

[46]
$$\beta = (1\ 2\cdots r) = (1\ r)(1\ r-1)\cdots(1\ 3)(1\ 2).$$ ■

每个置换都可以理解为一系列互换，但是这种分解不如分解为不相交轮换那样好．第一，对换未必交换：$(1\ 2\ 3) = (1\ 3)(1\ 2) \neq (1\ 2)(1\ 3)$；第二，无论因子本身还是因子的个数都不是唯一确定的．例如，下面 S_4 中 $(1\ 2\ 3)$ 的几种分解：

$$\begin{aligned}(1\ 2\ 3) &= (1\ 3)(1\ 2) \\ &= (2\ 3)(1\ 3) \\ &= (1\ 3)(4\ 2)(1\ 2)(1\ 4) \\ &= (1\ 3)(4\ 2)(1\ 2)(1\ 4)(2\ 3)(2\ 3).\end{aligned}$$

在这样的分解中还有那种唯一性？我们现在证明在置换 α 的一切分解中因子数目的奇偶性是不变的，即对换的个数恒为偶数或恒为奇数(如上面展示的 $\alpha = (1\ 2\ 3)$ 的分解).

例 2.11 **15 迷宫游戏**有一个**起始位置**，它是数 1 到 15 和叫做"白子"的符号 # 组成的 4×4 排阵．例如考虑下列起始位置：

3	15	4	8
10	11	1	9
2	5	13	12
6	7	14	#

交换白子和相邻的符号算作一步，例如从这个起始位置开始的第一步有两种选择：交换 # 和 14，

或者交换 # 和 12. 如果走了若干步之后，起始位置变成标准排阵 1,2,3,…,15,#，则游戏算赢.

为了分析该游戏，注意到给定的排阵其实是一个置换 $\alpha \in S_{16}$（如果现在把白子 # 叫做 16）. 更精确地说，如果小方块标以 1 到 16，则 $\alpha(i)$ 是第 i 个小方块上出现的符号. 例如给定的起始位置是

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 3 & 15 & 4 & 8 & 10 & 11 & 1 & 9 & 2 & 5 & 13 & 12 & 6 & 7 & 14 & 16 \end{pmatrix}.$$

每一步都是一个特殊类型的对换，即移动 16 的对换(记住现在白子是 16). 此外，从给定的位置(对应置换 β)走出一步(对应特殊对换 τ)产生一个新的位置对应置换 $\tau\beta$. 例如 α 是上面的位置，τ 是交换 14 和 16 的对换，则 $\tau\alpha(16) = \tau(16) = 14, \tau\alpha(15) = \tau(14) = 16$，而对其他所有的 $i, \tau\alpha(i) = i$. 就是说新的形状保留原先位置的所有的数，除了交换 14 和 16. 要赢得游戏需要特殊对换 $\tau_1, \tau_2, \cdots, \tau_m$ 使得

47

$$\tau_m \cdots \tau_2 \tau_1 \alpha = (1).$$

在例 2.15 中将会看到，对于 α 的某些取法，游戏可以赢，而对于另一些取法，游戏不可能赢. ■

定义 称置换 $\alpha \in S_n$ 为**偶置换**，如果它能分解为偶数个对换的乘积；否则称 α 为**奇置换**. 置换的**奇偶性**是指它是偶置换还是奇置换.

易知 (1 2 3) 和 (1) 是偶置换，因为对换分解 (1 2 3)=(1 3)(1 2) 和 (1)= (1 2)(1 2) 中有两个对换. 另一方面，我们尚无奇置换的例子！如果 α 是奇数个对换的乘积，也许它还有另一种分解，其中对换的个数为偶数. 毕竟奇置换的定义只是说 α 不能分解为偶数个对换的乘积.

定义 设 $\alpha \in S_n$ 且 $\alpha = \beta_1 \cdots \beta_t$ 是分解为不相交轮换的完全轮换分解. 定义 α 的**符号函数**为

$$\operatorname{sgn}(\alpha) = (-1)^{n-t}.$$

定理 2.3 表明 sgn 是(合理定义的)函数，因为数 t 由 α 唯一地确定. 注意对每个 1-轮换 ε，$\operatorname{sgn}(\varepsilon) = 1$，因为 $t = n$. 如果 τ 是对换，则它移动两个数而固定其他 $n-2$ 个数，所以，$t = (n-2)+1 = n-1$，从而 $\operatorname{sgn}(\tau) = (-1)^{n-(n-1)} = -1$.

定理 2.12 对所有 $\alpha, \beta \in S_n$，

$$\operatorname{sgn}(\alpha\beta) = \operatorname{sgn}(\alpha)\operatorname{sgn}(\beta).$$

证明概要 如果 $k, \ell \geqslant 0$ 且字母 a, b, c_j, d_j 都不同，则

$$(ab)(ac_1 \cdots c_k b d_1 \cdots d_\ell) = (ac_1 \cdots c_k)(bd_1 \cdots d_\ell);$$

这个等式左乘 (ab) 得

$$(ab)(ac_1 \cdots c_k)(bd_1 \cdots d_\ell) = (ac_1 \cdots c_k b d_1 \cdots d_\ell).$$

这些等式可用来证明对每个 $\alpha \in S_n, \operatorname{sgn}(\tau\alpha) = -\operatorname{sgn}(\alpha)$，其中 τ 是对换 (ab). 如果 $\alpha \in S_n$ 有对换分解 $\alpha = \tau_1 \cdots \tau_m$，其中每个 τ_i 是对换，可对 m 用归纳法证明对于每个 $\beta \in S_n, \operatorname{sgn}(\alpha\beta) = \operatorname{sgn}(\alpha)\operatorname{sgn}(\beta)$. ■

48

定理 2.13 (i) 设 $\alpha \in S_n$. 如果 $\operatorname{sgn}(\alpha) = 1$，则 α 是偶置换；如果 $\operatorname{sgn}(\alpha) = -1$，则 α 是奇置换.

(ii) 置换 α 是奇置换当且仅当它是奇数个对换的乘积.

证明 (i) 如果 $\alpha = \tau_1 \cdots \tau_q$ 是 α 的对换分解，则由定理 2.12，$\operatorname{sgn}(\alpha) = \operatorname{sgn}(\tau_1) \cdots \operatorname{sgn}(\tau_q) = (-1)^q$. 因此，如果 $\operatorname{sgn}(\alpha) = 1$，则 q 必定恒为偶数，如果 $\operatorname{sgn}(\alpha) = -1$，则 q 必定恒为奇数.

(ii) 如果 α 是奇置换，则 α 不是偶置换，于是 $\operatorname{sgn}(\alpha) \neq 1$，即 $\operatorname{sgn}(\alpha) = -1$. 现 $\alpha = \tau_1 \cdots \tau_q$，其中 τ_i 是对换，于是 $\operatorname{sgn}(\alpha) = -1 = (-1)^q$，因此 q 是奇数(我们已经证明了比定理更广的结果：α 的每个对换分解都有奇数个因子). 反之，如果 $\alpha = \tau_1 \cdots \tau_q$ 是对换乘积，其中 q 是奇数，则 $\operatorname{sgn}(\alpha) = -1$；所

以 α 不是偶置换，因此 α 是奇置换. ■

系 2.14 设 α，$\beta\in S_n$. 如果 α，β 有相同的奇偶性，则 $\alpha\beta$ 是偶置换；如果 α，β 的奇偶性不同，则 $\alpha\beta$ 是奇置换.

例 2.15 对例 2.11 中的 15 迷宫游戏的一个分析表明：如果 $\alpha\in S_{16}$ 是起始位置，则赢得游戏当且仅当 α 是固定 16 的偶置换. 关于这一点的一个证明读者可参考 McCoy-Janusz 所著的《Introduction to Morden Algebra》，229～234 页. 然而一个方向的证明是容易的. 开始时白子 16 在 16 的位置，每一步把 16 上移、下移、左移或右移. 移动总步数 m 为 $u+d+l+r$，其中 u 是上移的步数，等等. 如果 16 回到原处，则每一种移动法都必定复原，上移步数和下移步数一定相等（即 $u=d$），左移步数和右移步数也一定相等(即 $r=l$). 于是总步数是偶数：$m=2u+2r$，也就是说，如果 $\tau_m\cdots\tau_1\alpha=(1)$，则 m 是偶数. 因此 $\alpha=\tau_1\cdots\tau_m$（因为对于每个对换 τ，$\tau^{-1}=\tau$)，从而 α 是偶置换. 配备了这个定理，我们就知道起始位置 α 是奇置换不可能赢得游戏. 在例 2.11 中，

$$\alpha=(1\ 3\ 4\ 8\ 9\ 2\ 15\ 14\ 7)(5\ 10)(6\ 11\ 13)(12)(16)$$

[(12) 和 (16) 是 1-轮换]. 现在 $\mathrm{sgn}(\alpha)=(-1)^{16-5}=-1$，从而 α 是奇置换，所以不可能赢. ■

习题

2.1 设

$$\alpha=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\9&8&7&6&5&4&3&2&1\end{pmatrix},$$

49

求 $\mathrm{sgn}(\alpha)$ 和 α^{-1}.

2.2 如果 $\alpha\in S_n$，证明 $\mathrm{sgn}(\alpha^{-1})=\mathrm{sgn}(\alpha)$.

2.3 如果 $\sigma\in S_n$ 固定某个 j，其中 $1\leqslant j\leqslant n$ [即 $\sigma(j)=j$]. 定义 $\sigma'\in S_{n-1}$ 为对一切 $i\neq j$，$\sigma'(i)=\sigma(i)$. 证明

$$\mathrm{sgn}(\sigma')=\mathrm{sgn}(\sigma).$$

提示：用 σ 和 σ' 的完全轮换分解.

2.4 如果 $1\leqslant r\leqslant n$，证明在 S_n 中有

$$\frac{1}{r}[n(n-1)\cdots(n-r+1)]$$

个 r-轮换.

提示：任一 r-轮换有 r 种轮换记号.

2.5 (i) 如果 α 是 r-轮换，证明 $\alpha^r=(1)$.

提示：如果 $\alpha=(i_0\cdots i_{r-1})$，证明 $\alpha^k(i_0)=i_k$.

(ii) 如果 α 是 r-轮换，证明 r 是使得 $\alpha^k=(1)$的最小正整数 k.

提示：用命题 2.2.

2.6 证明 r-轮换是偶置换当且仅当 r 是奇数.

2.7 给定 $X=\{1,2,\cdots,n\}$，如果 X 的置换 τ 是形如 $(i,\ i+1)$ 的对换，其中 $i<n$，则称 τ 为**邻接对换**.

(i) 对 $n\geqslant 2$，S_n 中的每个置换都是邻接对换的乘积.

(ii) 设 $i<j$，证明 $(i\,j)$ 是奇数个邻接对换的乘积.

提示：对 $j-i$ 用归纳法.

2.8 定义 $f:\{0,1,2,\cdots,10\}\to\{0,1,2,\cdots,10\}$ 为

$$f(n)=4n^2-3n^7 \text{ 除以 11 的余数}.$$

(ⅰ)证明 f 是置换.[⊖]

(ⅱ)确定 f 是奇偶性.

(ⅲ)计算 f 的逆.

2.9 如果 α 是 r - 轮换且 $1 < k < r$,α^k 是 r - 轮换吗?

2.10 (ⅰ)证明:如果 α 和 β(不必不相交)是可交换的置换,则对一切 $k \geqslant 1$,$(\alpha\beta)^k = \alpha^k\beta^k$.

提示:先对 k 用归纳法证明 $\beta\alpha^k = \alpha^k\beta$.

(ⅱ)举出满足 $(\alpha\beta)^2 \neq \alpha^2\beta^2$ 的两个置换 α 和 β 的例子.

2.11 (ⅰ)证明对所有 i,$\alpha \in S_n$ 移动 i 当且仅当 α^{-1} 移动 i.

(ⅱ)证明:如果 $\alpha,\beta \in S_n$ 不相交且 $\alpha\beta = (1)$,则 $\alpha = (1)$,$\beta = (1)$.

2.12 证明 S_n 中偶置换的个数为 $\frac{1}{2}n!$.

提示:设 $\tau = (1\ 2)$,记 S_n 中全体偶置换的集合为 A_n,全体奇置换的集合为 O_n,定义 $f: A_n \to O_n$ 为

$$f: \alpha \mapsto \tau\alpha.$$

证明 f 是双射,于是 $|A_n| = |O_n|$,因此 $|A_n| = \frac{1}{2}n!$.

[50]

2.13 (ⅰ)在 S_5 中与 $\alpha = (1\ 2\ 3)$ 可交换的置换有多少?与 α 可交换的偶置换有多少?

提示:在 S_5 中有 6 个置换可与 α 交换,而偶置换只有 3 个.

(ⅱ)对 $(1\ 2)(3\ 4)$ 回答同样的问题.

提示:在 S_4 中有 8 个置换可与 $(1\ 2)(3\ 4)$ 交换,而偶置换只有 4 个.

2.14 举出 $\alpha,\beta,\gamma \in S_5$ 的一个例子,其中 $\alpha \neq (1)$,使其满足 $\alpha\beta = \beta\alpha$,$\alpha\gamma = \gamma\alpha$ 和 $\beta\gamma \neq \gamma\beta$.

2.15 设 $n \geqslant 3$.证明:如果 $\alpha \in S_n$ 和每个 $\beta \in S_n$ 可交换,则 $\alpha = (1)$.

2.16 如果 $\alpha = \beta_1 \cdots \beta_m$ 是不相交轮换的乘积,证明 $\gamma = \beta_1^{e_1} \cdots \beta_m^{e_m}\delta$ 与 α 可交换,其中对于一切 i,$e_i \geqslant 0$,并且 δ 与 α 不相交.

2.3 群

自伽罗瓦时代以来,除了对多项式根的研究外,还在数学的其他许多领域产生了群,正如我们将看到的,群是描述对称概念的一种方法.

"乘积"的核心是两个事物组合起来形成第三个同种事物.例如,通常的乘法、加法和减法都是把两个数结合起来给出另一个数,而复合把两个置换组合起来给出另一个置换.

定义 集合 G 上的**二元运算**是指函数

$$*: G \times G \to G.$$

更详细地说,一个二元运算对 G 中元素的每个有序对指定 G 中的一个元素 $*(x,y)$.把 $*(x,y)$ 写成 $x * y$ 是十分自然的.这样,函数的复合是函数 $(g,f) \mapsto g \circ f$,乘法、加法和减法分别是函数 $(x,y) \mapsto xy$,$(x,y) \mapsto x + y$ 和 $(x,y) \mapsto x - y$.复合和减法的例子说明我们为什么要强调有序对,因为 $x * y$ 和 $y * x$ 可能不同.和任意函数一样,二元运算是合理定义的,说得更清楚点,它满足通常所说的**代换定律**:

⊖ 假定 k 是有限域,则系数在 k 中的多项式称为**置换多项式**,如果由 $a \mapsto f(a)$ 定义的赋值函数 $f: k \to k$ 是 k 的置换.埃尔米特(Hermite)和迪克森(Dickson)的一个定理刻画了置换多项式(见 Lidl-Niederreiter 所著的《Introduction to Finite Fields and Their Applications》).

$$\text{如果 } x = x', y = y', \text{则 } x * y = x' * y'.$$

定义 群是指配置了二元运算 $*$ 的集合 G，且满足

（ⅰ）**结合律**成立：对每个 $x,y,z \in G$，

$$x * (y * z) = (x * y) * z.$$

（ⅱ）存在元素 $e \in G$，对一切 $x \in G$ 有 $e * x = x = x * e$，称 e 为**幺元**.

51

（ⅲ）每个 $x \in G$ 都有逆，即存在 $x' \in G$ 使得 $x * x' = e = x' * x$.

由定理 1.49，集合 X 上的一切置换的集合 S_X，连同作为运算的复合以及作为幺元的 $1_X = (1)$ 是群（X 上的**对称群**）. 在习题 2.22 中，读者会看到群定义中的有些等式是多余的，考察这一点有它的用处，因为当验证一个带有运算的集合确实是一个群的时候，所要核对的等式可以少一点，从而更有效.

我们现在正处在由代数转变为**抽象**代数的转折点上，与由 $\{1,2,\cdots,n\}$ 的全体置换构成的具体的群 S_n 相比，我们已经允许群的元素不是特别指定的，而且元素的乘积也不是明确地可计算的，而只是满足某些法则. 将会看到这一方法是卓有成效的，因为现在要把定理运用到许多不同的群上，只要一次性地证明就可以了，而不必对每一个不曾遇到过的群重新证明一次. 除明显的经济省事之外，从“抽象”角度展开的研究还往往比处理特定的、具体的群来得简单. 例如，我们会看到，不去识别论题中的元素是置换，S_n 中的某些性质反而更简单（见例 2.26）.

定义 如果群 G 满足**交换律**：对一切 $x,y \in G$，有

$$x * y = y * x,$$

则称 G 为**阿贝尔群**[㊀].

对 $n \geq 3$，群 S_n 不是阿贝尔群，因为 $(1\ 2)$ 和 $(1\ 3)$ 是 S_n 中的元素，它们不可交换：$(1\ 2)(1\ 3) = (1\ 3\ 2)$，而 $(1\ 3)(1\ 2) = (1\ 2\ 3)$.

引理 2.16 设 G 是群.

（ⅰ）**消去律**成立：如果 $x * a = x * b$ 或 $a * x = b * x$，则 $a = b$.

（ⅱ）e 是 G 中满足对一切 $x \in G$ 有 $e * x = x = x * e$ 的唯一元素.

（ⅲ）对每个 $x \in G$，x 的逆唯一：只有一个元素 $x' \in G$ 满足 $x * x' = e = x' * x$（因此记该元素为 x^{-1}）.

（ⅳ）对一切 $x \in G$，$(x^{-1})^{-1} = x$.

证明 （ⅰ）选取 x' 满足 $x' * x = e = x * x'$，则

$$\begin{aligned} a = e * a &= (x' * x) * a = x' * (x * a) \\ &= x' * (x * b) = (x' * x) * b = e * b = b. \end{aligned}$$

x 在右边时可类似地证明.

（ⅱ）设 $e_0 \in G$ 满足对一切 $x \in G$，$e_0 * x = x = x * e_0$，特别地，在第二个等式中取 $x = e$ 得

52

$e = e * e_0$. 另一方面，由 e 的定义得 $e * e_0 = e_0$，所以 $e = e_0$.

（ⅲ）假定 $x'' \in G$ 满足 $x * x'' = e = x'' * x$，等式 $e = x * x'$ 左乘 x'' 得

$$x'' = x'' * e = x'' * (x * x') = (x'' * x) * x' = e * x' = x'.$$

（ⅳ）由定义，$(x^{-1})^{-1} * x^{-1} = e = x^{-1} * (x^{-1})^{-1}$，而 $x * x^{-1} = e = x^{-1} * x$，根据（ⅲ），$(x^{-1})^{-1} = x$. ■

㊀ 交换群称为阿贝尔群的原因参见 236 页（这是指原书页码，与页边标注的页码一致，全书后同——编辑注）.

从现在起，通常用 xy 记群中的乘积 $x*y$（在对称群中已经用 $\alpha\beta$ 来简化 $\alpha\circ\beta$），并用 1 代替 e 来记幺元. 然而如果是阿贝尔群，则常用**加法记号** $x+y$，此时幺元记为 0，元素 x 的逆记为 $-x$ 以代替 x^{-1}.

例 2.17 （i）全体非零有理数的集合 $\mathbb{Q}^{\times}$ 是阿贝尔群，其中 $*$ 是通常乘法，数 1 是幺元，$r\in\mathbb{Q}^{\times}$ 的逆是 $1/r$. 类似地，$\mathbb{R}^{\times}$ 和 $\mathbb{C}^{\times}$ 也是乘法阿贝尔群.

注意全体非零整数的集合 $\mathbb{Z}^{\times}$ 不是乘法群，因为它没有一个元素（除了 ± 1）在乘法下的逆是整数.

（ii）全体整数的集合 $\mathbb{Z}$ 是加法阿贝尔群，其中 $a*b=a+b$，幺元 $e=0$，整数 n 的逆是 $-n$. 同样可知，$\mathbb{Q}$，$\mathbb{R}$ 和 $\mathbb{C}$ 也是加法阿贝尔群.

（iii）**圆群**

$$S^1=\{z\in\mathbb{C}:|z|=1\}$$

是群，其运算是复数的乘法，该乘法所以称为运算是根据系 1.31，模 1 复数的乘积依然模 1. 复数乘法是结合的，幺元是 1（它的模为 1），任一模 1 复数的逆是它的复共轭，其模也是 1. 所以 S^1 是群.

（iv）对任意正整数 n，设

$$\mu_n=\{\zeta^k:0\leqslant k<n\}$$

是全体 n 次单位根的集合，其中

$$\zeta=e^{2\pi i/n}=\cos\left(\frac{2\pi}{n}\right)+i\sin\left(\frac{2\pi}{n}\right).$$

读者可由棣莫弗定理获知 μ_n 是带复数乘法运算的群. 此外，任一 n 次单位根的逆是它的复共轭，也是 n 次单位根.

53

（v）平面 $\mathbb{R}\times\mathbb{R}$ 是带向量加法的群；即如果 $\alpha=(x,y)$，$\alpha'=(x',y')$，则 $\alpha+\alpha'=(x+x',y+y')$. 幺元是原点 $O=(0,0)$，(x,y) 的逆是 $(-x,-y)$. ■

例 2.18 设 X 是集合，U，V 是 X 的子集. 定义

$$U-V=\{x\in U:x\notin V\}.$$

布尔群 $\mathcal{B}(X)$［以逻辑学家布尔（G. Boole，1815—1864）的名字命名］是 X 的全体子集的族，它配置了由**对称差**给出的加法 $A+B$，其中

$$A+B=(A-B)\cup(B-A);$$

图 2.2 是对称差的图示.

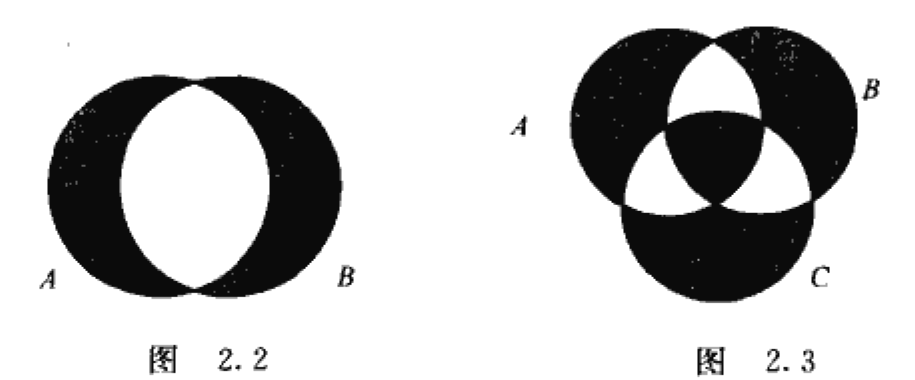


图 2.2　　　图 2.3

显然 $A+B=B+A$，因此对称差是交换的. 幺元是空集 $\varnothing$，A 的逆是 A 自身，因为 $A+A=\varnothing$. 读者可以证明 $(A+B)+C$ 和 $A+(B+C)$ 两者都是如图 2.3 所描画的形状，从而验证结合律. ■

例 2.19 一个 $n\times n$ 实数矩阵如果有逆则称为**非奇异的**；即存在矩阵 B 使得 $AB=I=BA$，其中 $I=[\delta_{ij}]$（δ_{ij} 是克罗内克 δ）是 $n\times n$ 单位矩阵. 因 $(AB)^{-1}=B^{-1}A^{-1}$，所以非奇异矩阵的乘积

也是非奇异的. 全体 $n \times n$ 非奇异实数矩阵的集合 $\mathrm{GL}(n,\mathbb{R})$ 连同二元运算矩阵乘法是(非阿贝尔)群，称为**一般线性群**. [结合律的证明虽然繁琐，却是平淡的，一旦了解了矩阵和线性变换间的关系之后，便可以给出简洁的证明(系 3.99).] ■

54

二元运算允许一次乘两个元素，那么三个元素怎样相乘？有一种选择，例如给出一个表达式 $2\times3\times4$，可以先做乘法 $2\times3=6$，再做 $6\times4=24$，也可以先做乘法 $3\times4=12$，再做 $2\times12=24$. 当然答案是一样的，因为数的乘法是结合的. 由此，如果一个运算是结合的，则表达式 abc 无歧义. 然而，并非所有运算都是结合的，例如减法就不是结合的：如果 $c\neq0$，则

$$a-(b-c)\neq(a-b)-c,$$

因此记号 $a-b-c$ 是有歧义的. $\mathbb{R}^3$ 中两向量的叉积是非结合运算的另一个例子.

定义 设 G 是群，$a\in G$. 对 $n\geqslant1$，归纳定义幂[⊖] a^n：

$$a^1=a,\quad a^{n+1}=aa^n.$$

定义 $a^0=1$. 如果 n 是正整数，定义

$$a^{-n}=(a^{-1})^n.$$

读者期望 $(a^{-1})^n=(a^n)^{-1}$，这是习题 2.17 中等式的特殊情形，而现阶段证明这一点并非想象中的那样明显. 例如证明 $a^{-2}a^2=1$ 相当于在表达式 $(a^{-1}a^{-1})(aa)$ 中作抵消，但是结合性是对三个因子的乘积给出的，而不是四个.

回到幂. 一次和二次幂是清楚的：$a^1=a$，$a^2=aa$. 立方有两种可能：已经定义了 $a^3=aa^2=a(aa)$，但还有一种合乎情理的竞选者：$(aa)a=a^2a$. 如果我们假定了结合性，则两者相等：

$$a^3=aa^2=a(aa)=(aa)a=a^2a.$$

a 的四次自乘有好几种可能性，假定运算是结合的，$a^4=a^3a=a^2a^2$ 是明显的吗？更高次幂又怎样？

定义**表达式** $a_1a_2\cdots a_n$ 为 $G\times\cdots\times G$ (n 个因子)中的一个 n 元组. 用下面的方法，一个表达式可产生 G 中的许多元素. 选取两个相邻的 a 相乘，得 $n-1$ 个因子的表达式：即刚形成的新乘积和原来的 $n-2$ 个因子. 在缩短的表达式中，再选取两个相邻因子(要么是原来的一对，要么一个是原来的，另一个是第一步形成的新乘积)相乘. 重复此法直到只有两个因子的表达式；最后把它们相乘得 G 中的一个元素；称这个元素为由表达式导出的一个**最终乘积**. 例如，考虑表达式 $abcd$，可以先乘 ab 得表达式 $(ab)cd$，它有三个因子，即 ab，c 和 d. 现在可选取 c，d 为一对，或选 ab,c 为一对，相乘得到两个因子的表达式：有因子 ab 和 cd 的表达式 $(ab)(cd)$，或有因子 $(ab)c$ 和 d 的表达式 $((ab)c)d$. 不论哪种选取法，把最后的表达式中的两个因子相乘，可得到由 $abcd$ 导出的最终乘积. 由表达式 $abcd$ 导出的其他最终乘积来自第一步取 b，c 相乘，或取 c，d 相乘. 从给定的表达式导出的最终乘积是否都相等并不是明显的.

55

定义 称一个表达式 $a_1a_2\cdots a_n$ **不需加括号**，如果它导出的一切最终乘积都相等，即不论选取怎样的相邻因子相乘，在 G 中的最终乘积都相等.

⊖ x^2 和 x^3 的术语 x 平方和 x 立方当然起源于几何. 在这个背景中字 power（幂）的用法是由于欧几里得使用的希腊字 dunamis（驱动机器的动力）被误译造成的. Power 是 dunamis 的标准欧洲翻版，例如 1570 年比林斯利（H. Billingsley）翻译的最早的欧几里得英语版，把欧几里得的一个句子翻译为"直线的 power 是同一直线的平方". 然而，欧几里得的同时代人（如亚里士多德（Aristotle）和柏拉图（Plato））常用 dunamis 表示扩大，似乎这是更合适的翻译，因为欧几里得可能的想法是：一维直线的滑移形成一个二维方形.（感谢 Donna Shalev 告诉我 dunamis 的古典用法.）

定理 2.20(广义结合性) 设 G 是群，$a_1, a_2, \cdots, a_n \in G$，则表达式 $a_1 a_2 \cdots a_n$ 不需加括号.

注 该结果在更广的范围内成立，因为证明中既不用幺元也不用逆.

证明 用归纳法(第二归纳法)证明. 基础步 $n=3$ 来自结合性. 关于归纳步，考虑经两种序列选择后从表达式 $a_1 a_2 \cdots a_n$ 得到的两个最终乘积 U 和 V：

$$(a_1 \cdots a_i)(a_{i+1} \cdots a_n), (a_1 \cdots a_j)(a_{j+1} \cdots a_n);$$

括号表示最后的两个因子，它们相乘得 U 和 V，在这些短表达式中还包含许多括号. 可假定 $i \leqslant j$. 因为括号中四个表达式的每一个所包含的因子都少于 n，所以归纳假设说它们都不需加括号. 由此，如果 $i = j$，则 $U = V$. 如果 $i < j$，则归纳假设允许把第一个表达式重写为

$$U = (a_1 \cdots a_i)([a_{i+1} \cdots a_j][a_{j+1} \cdots a_n])$$

把第二个表达式重写为

$$V = ([a_1 \cdots a_i][a_{i+1} \cdots a_j])(a_{j+1} \cdots a_n),$$

其中每一个表达式 $a_1 \cdots a_i, a_{i+1} \cdots a_j$ 和 $a_{j+1} \cdots a_n$ 都不需加括号，于是这些表达式分别产生 G 的唯一元素 A, B 和 C. 第一个表达式产生 $A(BC)$，第二个表达式产生 $(AB)C$，由结合性，这两个表达式给出 G 的同一元素. ■ [56]

系 2.21 设 G 是群，$a, b \in G$，则

$$(ab)^{-1} = b^{-1} a^{-1}.$$

证明 根据引理 2.16(ⅲ)，只需证明 $(ab)(b^{-1}a^{-1}) = 1 = (b^{-1}a^{-1})(ab)$. 用广义结合性得

$$(ab)(b^{-1}a^{-1}) = [a(bb^{-1})]a^{-1} = (a1)a^{-1} = aa^{-1} = 1.$$

另一等式可以类似地证明. ■

系 2.22 设 G 是群. 如果 $a \in G$ 且 $m, n \geqslant 1$，则

$$a^{m+n} = a^m a^n, (a^m)^n = a^{mn}.$$

证明 第一种情形，两个元素均来自有 $m+n$ 个因子且每个因子都等于 a 的表达式. 第二种情形，两个元素均来自有 mn 个因子且每个因子都等于 a 的表达式. ■

由此，群中元素 a 的任两个幂可交换：

$$a^m a^n = a^{m+n} = a^{n+m} = a^n a^m.$$

命题 2.23(指数定律) 设 G 是群，$a, b \in G$ 且 m 和 n (不必是正的) 是整数.

(ⅰ) 如果 a 和 b 可交换，则 $(ab)^n = a^n b^n$.

(ⅱ) $(a^n)^m = a^{mn}$.

(ⅲ) $a^m a^n = a^{m+n}$.

证明概要 证明是冗长的双重归纳法，然而是平淡的. ■

记号 a^n 是表示 $a * a * \cdots * a$ (其中 a 出现 n 次)的自然方式，然而，如果运算是+，则更自然的是记 $a + a + \cdots + a$ 为 na. 设 G 是写作加法的群，$a, b \in G$，且 m, n (不必是正的)是整数，则命题 2.23 通常写作：

(ⅰ) $n(a+b) = na + nb$.

(ⅱ) $m(na) = (mn)a$.

(ⅲ) $ma + na = (m+n)a$. [57]

定义 设 G 是群，$a \in G$. 如果对某个 $k \geqslant 1$ 有 $a^k = 1$，则这样的最小指数 $k \geqslant 1$ 称为 a 的**阶**. 如果没有这样的幂存在，则称 a 的**阶无限**.

整数的加法群 $\mathbb{Z}$ 是群，3 是其中的一个元素，其阶无限(因 $3+3+\cdots+3$ 永不为 0).

在任一群中，幺元的阶为1，且它是阶为1的唯一元素．一个元素的阶为2当且仅当它和它的逆相等.

阶的定义说，如果x的阶为n且有某个正整数m使得$x^m=1$，则$n\leqslant m$．下一定理说n必是m的因数.

定理 2.24 *如果$a\in G$是n阶元素，则$a^m=1$当且仅当$n\mid m$.*

证明 假定$a^m=1$．带余除法给出整数q和r使得$m=qn+r$，其中$0\leqslant r<n$．由此$a^r=a^{m-nq}=a^m a^{-nq}=1$．如果$r>0$，则与$n$是使得$a^n=1$的最小正整数矛盾，因此$r=0$且即$n\mid m$．反之，如果$m=nk$，则$a^m=a^{nk}=(a^n)^k=1^k=1$ ■.

S_n中的置换的阶是什么?

命题 2.25 *设$\alpha\in S_n$.*

(i) 如果α是r－轮换，则α的阶为r.

(ii) 如果$\alpha=\beta_1\cdots\beta_t$是不相交的$r_i$－轮换$\beta_i$的积，则$\alpha$的阶为$\mathrm{lcm}\{r_1,\cdots,r_t\}$.

(iii) 如果p是素数，则α的阶为p当且仅当α是一个p－轮换或是不相交p－轮换的积.

证明 (i) 这是习题2.5.

(ii) 由(i)，每个β_i的阶为r_i．假设$\alpha^M=(1)$，因β_i可交换，$(1)=\alpha^M=(\beta_1\cdots\beta_t)^M=\beta_1^M\cdots\beta_t^M$．由习题2.11，各$\beta$不相交蕴涵对每个$i,\beta_i^M=(1)$，根据定理2.24，对一切$i,r_i\mid M$；即$M$是$r_1,\cdots,r_t$的公倍数．另一方面，如果$m=\mathrm{lcm}\{r_1,\cdots,r_t\}$，则易知$\alpha^m=(1)$．所以$\alpha$的阶为$m$.

(iii) 把α写作不相交轮换的积，再用(ii). ■

举例来说，S_n中一个置换的阶为2当且仅当它是一个对换或不相交对换的积.

例 2.26 假定洗一次扑克牌把顺序1,2,3,4，…，52变成2,1,4,3,…，52,51，如果用同样方式再洗一次，则扑克牌又回到原来的顺序．对52张牌的任一置换α也会发生同样的情形：把α重复充分多次，最终牌局回到原来的顺序．要了解其原因的一种方法是运用我们的置换知识．把α写作不相交轮换的积，比如$\alpha=\beta_1\beta_2\cdots\beta_t$，其中$\beta_i$是$r_i$－轮换．由命题2.25，$\alpha$的阶为$k$，其中$k$是$r_i$的最小公倍数．所以$\alpha^k=(1)$.

58

可用更简单的证明方法得到更一般的结果(抽象代数比代数更容易)：设G是有限群，$a\in G$，则有某个$k\geqslant1$使得$a^k=1$．考虑子集$\{1,a,a^2,\cdots a^n,\cdots\}$．因$G$有限，在此无限表中必有重复，即有整数$m>n$满足$a^m=a^n$，因此$1=a^m a^{-n}=a^{m-n}$，于是证明了$a$的某个正幂等于1．[原先对于52张牌的置换$\alpha$所作的论证不是无用的，因为它给出了计算$k$的算法.] ■

把例2.26中刚证明的结果陈述如下：

命题 2.27 *如果G是有限群，则每个$x\in G$的阶都有限.*

表2.3讨论了例2.5(ii)中的表.

表 2.3 S_5中的置换

轮换结构	个数	阶	奇偶性
(1)	1	1	偶
(1 2)	10	2	奇
(1 2 3)	20	3	偶
(1 2 3 4)	30	4	奇
(1 2 3 4 5)	24	5	偶
(1 2)(3 4 5)	20	6	奇
(1 2)(3 4)	15	2	偶
	120		

下面是群的几个几何例子.

定义 称保持距离的双射 $\varphi: \mathbb{R}^2 \to \mathbb{R}^2$ [可以证明如果 $\varphi(0)=0$，则 φ 是线性变换] 为**运动**. 如果 π 是平面上的多边形，则 π 的**对称群** $\Sigma(\pi)$ 由满足 $\varphi(\pi)=\pi$ 的一切运动 φ 组成，$\Sigma(\pi)$ 的元素称做 π 的**对称**.

例 2.28 (i) 设 π_4 是边长为 1，顶点为 $\{v_1, v_2, v_3, v_4\}$ 的正方形. 在平面上画出 π_4 使其中心在原点、边平行于坐标轴. 可以证明每个 $\varphi \in \Sigma(\pi_4)$ 置换各顶点. 确实，π_4 的一个对称 φ 由 $\{\varphi(v_i): 1 \leqslant i \leqslant 4\}$ 所确定，由此最多有 $24=4!$ 个可能的对称. 然而 S_4 中的所有置换并非都是 π_4 的对称. 如果 v_i 和 v_j 相邻，则 $\| v_i - v_j \| = 1$，而 $\| v_1 - v_3 \| = \sqrt{2} = \| v_2 - v_4 \|$，由此 φ 必保持相邻性(因为运动保持距离). 读者可验证 π_4 的对称只有 8 个，除了恒等函数和绕 O 旋转 90°、180°和 270°之外，还有关于直线 v_1v_3 和 v_2v_4 以及 x 轴和 y 轴四个反射(为了将来的推广，注意 y 轴是 Om_1，m_1 是 v_1v_2 的中点，x 轴是 Om_2，m_2 是 v_2v_3 的中点). 群 $\Sigma(\pi_4)$ 称为有 8 个元素的**二面体群**㊀，记为 D_8.

59

(ii) 中心在 O、顶点为 v_1，v_2，v_3，v_4，v_5 的正五边形 π_5 的对称群 $\Sigma(\pi_5)$ 有 10 个元素：绕原点旋转 $(72j)°$，其中 $0 \leqslant j \leqslant 4$，以及关于直线 $Ov_k (1 \leqslant k \leqslant 5)$ 的反射. 对称群 $\Sigma(\pi_5)$ 称作有 10 个元素的**二面体群**，记为 D_{10}. ■

定义 设 π_n 是中心在 O、n 个顶点为 $v_1, v_2, \cdots, v_n$ 的正多边形. 称对称群 $\Sigma(\pi_n)$ 为有 $2n$ 个元素的**二面体群**，记为㊁ D_{2n}.

二面体群 D_{2n} 包括绕中心的 n 个 $(360j/n)°$旋转 $\rho^j, 0 \leqslant j \leqslant n-1$. 描述其他 n 个元素要依赖 n 的奇偶性. 如果 n 是奇数(如五边形的情形，见图 2.5)，则这 n 个对称是关于不同直线 $Ov_i (i=1, 2, \cdots, n)$ 的反射. 如果 $n=2q$ 是偶数(见图 2.4 的正方形，或图 2.6 的正六边形)，则直线 Ov_i 与直线 Ov_{q+i} 相同，只能得到 q 个这样的反射，剩下的 q 个对称是关于直线 $Om_i (i=1,2,\cdots,q)$ 的反射，其中 m_i 是边 v_iv_{i+1} 的中点. 例如，π_6 的六条对称直线是 Ov_1, Ov_2, Ov_3 和 Om_1, Om_2, Om_3.

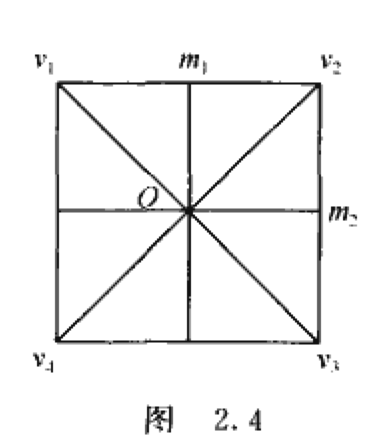


图 2.4

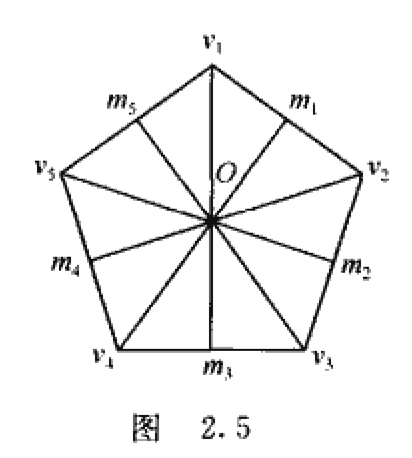


图 2.5

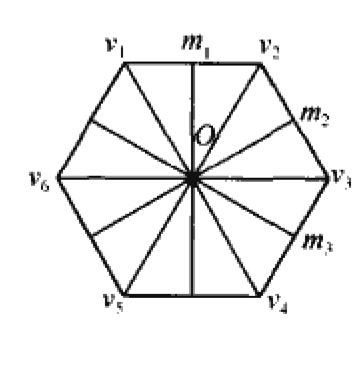


图 2.6

习题

2.17 如果 $a_1, a_2, \cdots, a_{t-1}, a_t$ 是群 G 中的元素，证明

㊀ 克莱因 (F. Klein) 研究了那些作为 $\mathbb{R}^3$ 的运动群的子群出现的有限群，其中有一些是作为正多面体的对称群出现的 [polyhedra(多面体)源自意为“多”的 Poly 和意为“二维边界”的 hedron 的希腊语]. 他发现一个退化的多面体，称之为 dihedron(二面体)，源自意为“二”的希腊字 di 和希腊字 hedron，它表示由两个零厚度的全等多边形粘合而成的形状. 二面体的对称群由此称为二面体群. 对我们来说，如课文那样描述这些群更自然.

㊁ 有些作者记 D_{2n} 为 D_n.

$$(a_1 a_2 \cdots a_{t-1} a_t)^{-1} = a_t^{-1} a_{t-1}^{-1} \cdots a_2^{-1} a_1^{-1}.$$

2.18 假定 G 是带有结合的二元运算的集合，不用广义结合性来证明 $(ab)(cd) = a[(bc)d]$.

2.19 (i) 计算

$$\alpha = (1\ 2)(4\ 3)(1\ 3\ 5\ 4\ 2)(1\ 5)(1\ 3)(2\ 3)$$

的阶、逆和奇偶性.

(ii) 习题 2.1 和习题 2.8 中的置换的阶各是什么?

2.20 (i) 在 S_5 和 S_6 中 2 阶元素有多少?

(ii) S_n 中 2 阶元素有多少?

提示：可用和式来表示答案.

2.21 如果 G 是群，证明满足 $g^2 = g$ 的唯一元素 $g \in G$ 是 1.

2.22 本题用较少的公理来定义群. 设 H 是包含元素 e 的集合，且假定在 H 上有结合的二元运算 $*$ 满足下列性质：

1. 对一切 $x \in H, e * x = x$.

2. 对每个 $x \in H$，存在 $x' \in H$ 使得 $x' * x = e$.

(i) 证明：如果 $h \in H$ 满足 $h * h = h$，则 $h = e$.

提示：如果 $h' * h = e$，用两种方法计算 $h' * h * h$.

(ii) 证明：对所有 $x \in H, x * x' = e$.

提示：考虑 $(x * x')^2$.

60 ~ 61

(iii) 证明：对所有 $x \in H, x * e = x$.

提示：用两种方法计算 $x * x' * x$.

(iv) 证明：如果 $e' \in H$ 满足对所有的 $x \in H$ 有 $e' * x = x$，则 $e' = e$.

提示：证明 $(e')^2 = e'$.

(v) 设 $x \in H$. 证明：如果 $x'' \in H$ 满足 $x'' * x = e$，则 $x'' = x'$.

提示：用两种方法计算 $x' * x * x''$.

(vi) 证明 H 是群.

2.23 设 y 是阶为 m 的群元素，如果对某个素数 p 有 $m = pt$，证明 y^t 的阶为 p.

提示：显然有 $(y^t)^p = 1$. 用定理 2.24 证明 y^t 没有更小的幂等于 1.

2.24 设 G 是群，$a \in G$ 的阶为 k. 如果 p 是 k 的素因数，且有 $x \in G$ 满足 $x^p = a$，证明 x 的阶为 pk.

2.25 设 $G=\mathrm{GL}(2, \mathbb{Q})$，并设

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \qquad B = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}.$$

证明 $A^4 = I = B^6$，而对一切 $n > 0, (AB)^n \neq I$，其中 $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ 是 2×2 单位矩阵. 由此可知 AB 的阶无限，即使它的两个因子 A 和 B 的阶都有限(在有限群中不可能出现这种情形).

2.26 如果 G 是群，且对每个 $x \in G$ 有 $x^2 = 1$，证明 G 必是阿贝尔群 [例 2.18 中的布尔群 $\mathcal{B}(X)$ 就是这样的群].

2.27 如果 G 是有偶数个元素的群，证明 G 中 2 阶元素的个数是奇数，特别地，G 至少包含一个 2 阶元素.

提示：把每个元素和它的逆配对.

2.28 S_n 中阶最大的元素是什么? 其中 $n = 1,2,\cdots,10$ [我们注明尚不知道对于任意 n 的一般公式，虽然 1903 年兰道 (E. Landau) 发现了渐近状态].

2.4 拉格朗日定理

群 G 的子群 H 是包含在 G 中的群，如果 $h,h' \in H$，则 H 中的积 hh' 和 G 中的积 hh' 相同. 然而，为了用起来更方便还是给出子群的正式定义.

定义 称群 G 的子集 H 为**子群**，如果

(i) $1 \in H$；

(ii) 如果 $x,y \in H$，则 $xy \in H$；

(iii) 如果 $x \in H, x^{-1} \in H$.

如果 H 是 G 的子群，则记为 $H \leqslant G$；如果 H 是 G 的真子群，即 $H \neq G$，则记为 $H < G$.

62

$\{1\}$ 和 G 恒为 G 的子群，其中 $\{1\}$ 是由一个元素 1 组成的子集. 更为重要的例子将立即给出. 子群 $H \neq G$ 称为**真子群**.

每个子群 $H \leqslant G$ 自身也是群. 性质 (ii) 表明 H 是**封闭的**；即 H 有二元运算. 结合性 $(xy)z = x(yz)$ 对一切 $x,y,z \in G$ 成立，从而特别对一切 $x,y,z \in H$ 也成立. 最后 (i) 给出了幺元，(iii) 给出了逆.

验证群 G 的子集 H 是子群(因而 H 自身是群)比验证 H 满足群公理容易：已从 G 上的运算继承了结合性，不需再验证.

例 2.29 (i) 四个置换

$$\mathbf{V} = \{(1),(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}$$

形成一个群，因为 $\mathbf{V}$ 是 S_4 的子群：$(1) \in \mathbf{V}$；对每个 $\alpha \in \mathbf{V}, \alpha^2 = (1)$，由此 $\alpha^{-1} = \alpha \in \mathbf{V}$；$\mathbf{V} - (1)$ 中任两个不同置换的乘积是第三个置换. 称群 $\mathbf{V}$ 为**四群**($\mathbf{V}$ 是原先德语术语 Vierergruppe 的缩写).

看看验证结合性 $a(bc) = (ab)c$ 要陷入怎样的麻烦：每个 a,b,c 都有四种选择，因此有 $4^3 = 64$ 个等式需要验证. 显然证明 $\mathbf{V}$ 是群的最好方法是证明它是 S_4 的子群.

(ii) 如果把平面 $\mathbb{R}^2$ 看作(加法)阿贝尔群，则过原点的任一直线 L 是一个子群. 最容易的验证方法是在 L 上选取一点 $(a,b) \neq (0,0)$，并注意 L 由一切标量乘积 (ra,rb) 组成. 读者现在可验证定义子群的公理对 L 成立. ■

可用较少的项目来验证一个子集确实是一个子群.

命题 2.30 群 G 的子集 H 是子群当且仅当 H 非空，且当 $x,y \in H$ 时，$xy^{-1} \in H$.

证明 必要性显然成立. 关于充分性，取 $x \in H$(因 $H \neq \varnothing$，所以必能取到). 由假设，$1 = xx^{-1} \in H$. 如果 $y \in H$，则 $y^{-1} = 1y^{-1} \in H$. 而如果 $x,y \in H$，则 $xy = x(y^{-1})^{-1} \in H$. ■

自然，验证一个子群的候选者 H 非空的最简单方法是看是否有 $1 \in H$.

注意，如果 G 中的运算是加法，则上一命题的条件是：H 是非空子集且满足 $x,y \in H$ 蕴涵 $x - y \in H$.

命题 2.31 有限群 G 的非空子集 H 是子群当且仅当 H 是闭的；即如果 $a,b \in H$，则 $ab \in H$. 特别地，S_n 的非空子集是子群当且仅当它是闭的.

63

证明概要 因 G 有限，命题 2.27 说每个 $x \in G$ 的阶有限，因此，如果 $x^n = 1$，则 $1 \in H$ 且 $x^{-1} = x^{n-1} \in H$. ■

上面的命题当 G 是无限群时可能不成立. 例如，设 G 是加法群 $\mathbb{Z}$，子集 $H = \mathbb{N}$ 是闭的，但不是 $\mathbb{Z}$ 的子群.

在 1830 年，对伽罗瓦来说群是在复合下封闭的 S_n 的子集 H；即如果 $\alpha,\beta\in H$，则 $\alpha\beta\in H$. 1854 年，凯莱（A. Cayley）第一次定义了抽象群，明确提出了结合性、逆和幺元，然后他证明(见凯莱定理)每个有 n 个元素的抽象群本质上是 S_n 的子群(下一节引入了同构的概念后可以给出更精确的陈述).

例 2.32 由一切偶置换组成的 S_n 的子集 A_n 是子群，因为它在乘法下封闭：偶∘偶=偶. 这个子群 $A_n\leqslant S_n$ 称为 n 个字母上的**交错**[㊀]**群**. ■

定义 如果 G 是群，且 $a\in G$，记

$$\langle a\rangle=\{a^n: n\in\mathbb{Z}\}=\{a \text{ 的一切幂}\}.$$

$\langle a\rangle$称为 G 的由 a **生成的循环子群**. 群 G 称为**循环群**，如果存在 $a\in G$ 使得 $G=\langle a\rangle$，此时称 a 为 G 的**生成元**.

易知$\langle a\rangle$确实是一个子群：$1=a^0\in\langle a\rangle$；$a^na^m=a^{n+m}\in\langle a\rangle$；$a^{-1}\in\langle a\rangle$. 例2.17(iv)表明，对每个 $n\geqslant1$，全体 n 次单位根的乘法群 μ_n 是循环群，它以 n 次单位原根 $\zeta=e^{2\pi i/n}$ 为生成元.

无疑，在早先的课程中读者已经知道整数模 m 的例子，我们仅回顾它的定义. 给定 $m\geqslant0$ 和 $a\in\mathbb{Z}$，$a \bmod m$ 的同余类 $[a]$ 定义如下：

$$\begin{aligned}[a]&=\{b\in\mathbb{Z}: b\equiv a \bmod m\}\\&=\{a+km: k\in\mathbb{Z}\}\\&=\{\cdots,a-2m,a-m,a,a+m,a+2m,\cdots\}.\end{aligned}$$

64

定义 **整数 mod m** 是指 mod m 的一切同余类的族，记为[㊁]$\mathbb{I}_m$.

回忆在$\mathbb{I}_m$ 中$[a]=[b]$当且仅当$a\equiv b\bmod m$. 特别地，在$\mathbb{I}_m$ 中$[a]=[0]$当且仅当$a\equiv0\bmod m$；即在$\mathbb{I}_m$ 中$[a]=[0]$当且仅当 m 是 a 的因数. mod$m$ 同余的定义对一切 $m\geqslant0$ 都有意义，但 $m=0$ 和 $m=1$ 的情形没有什么意思：$a\equiv b\bmod 0$ 意味着 $0\mid(a-b)$，就是说 $a=b$；$a\equiv b\bmod 1$ 意味着 $1\mid(a-b)$，就是说 a 和 b 总是同余的，即只有一个 mod 1 的同余类. 回顾命题 1.19，我们现在用方括号的记号重写如下.

命题 1.19 设 $m\geqslant2$ 是固定的整数.

(i) 如果 $a\in\mathbb{Z}$，则有某个 r 满足 $0\leqslant r<m$ 使得 $[a]=[r]$.

(ii) 如果 $0\leqslant r'<r<m$，则 $[r']\neq[r]$.

(iii) $\mathbb{I}_m$ 恰有 m 个元素，即 $[0],[1],\cdots,[m-1]$.

对每个 $m\geqslant2$，$\mathbb{I}_m$是(加法)循环群，其中

$$[a]+[b]=[a+b];$$

幺元是$[0]$,$[a]$的逆是$[-a]$，生成元是 $[1]$. (iii) 表明$\mathbb{I}_m$ 的阶为 m.

循环群可以有好几个不同的生成元，如$\langle a\rangle=\langle a^{-1}\rangle$.

㊀ 在研究多项式时第一次产生了交错群. 如果

$$f(x)=(x-u_1)(x-u_2)\cdots(x-u_n),$$

则数 $D=\prod_{i<j}(u_i-u_j)$ 随根的排列而改变符号：如果 α 是 $\{u_1,u_2,\cdots,u_n\}$ 的一个置换，易知 $\prod_{i<j}[\alpha(u_i)-\alpha(u_j)]=\pm D$. 当各种置换 α 作用到 D 的因子上时，这个积交替变换符号，但对于交错群中的那些 α 符号不变. 后一事实可用来给出定理 2.13 (ii) 的另一个证明.

㊁ 引入新记号是因为没有一致认同的记号，最大众化的是$\mathbb{Z}_m$ 和$\mathbb{Z}/m\mathbb{Z}$. 选择$\mathbb{I}_m$ 是因为 I 是 integers(整数)的起首字母. 整数的通常记号是$\mathbb{Z}$(它是德语 Zahlen 的起首字母)，这几乎是一致公认的. 因此从$\mathbb{Z}$变到$\mathbb{I}$是连贯的，不致太迷茫.

定理 2.33 (i) 如果 $G=\langle a\rangle$ 是 n 阶循环群，则 a^k 是 G 的生成元当且仅当 $(k,n)=1$.

(ii) 如果 G 是 n 阶循环群，记 $\text{gen}(G)=\{G\text{ 的所有生成元}\}$，则

$$|\text{gen}(G)|=\phi(n),$$

其中 ϕ 是欧拉 ϕ-函数.

证明 (i) 如果 a^k 生成 G，则 $a\in\langle a^k\rangle$，因此有某个 $t\in\mathbb{Z}$ 使得 $a=a^{kt}$，从而 $a^{kt-1}=1$. 根据定理 2.24, $n\mid(kt-1)$，由此存在 $v\in\mathbb{Z}$ 使得 $nv=kt-1$，因此 1 是 k 和 n 的线性组合，于是 $(k,n)=1$.

反之，如果 $(k,n)=1$，则有 $t,u\in\mathbb{Z}$ 使得 $nt+ku=1$，因此

$$a=a^{nt+ku}=a^{nt}a^{ku}=a^{ku}\in\langle a^k\rangle.$$

所以 a 的每个幂都在 $\langle a^k\rangle$ 中，即 $G=\langle a^k\rangle$.

(ii) 命题 1.38 说 $\phi(n)=|\{k\leqslant n:(k,n)=1\}|$. 下一命题将证明 $G=\{1,a,\cdots,a^{n-1}\}$，从而由 (i) 可得结论. ■

65

命题 2.34 设 G 是有限群，$a\in G$，则 a 的阶为 $|\langle a\rangle|$，它是 $\langle a\rangle$ 中元素的个数.

证明 因 G 是有限的，因此存在整数 $k\geqslant 1$ 使得 $1,a,a^2,\cdots,a^{k-1}$ 各不相同，而 $1,a,a^2,\cdots,a^k$ 有重复，因此 $a^k\in\{1,a,a^2,\cdots,a^{k-1}\}$，即有某个 i 满足 $0\leqslant i<k$ 使得 $a^k=a^i$. 如果 $i\geqslant 1$，则 $a^{k-i}=1$，这与第一个数列没有重复元素相矛盾，所以 $a^k=a^0=1$ 且 k 是 a 的阶(满足该式的最小正整数).

如果 $H=\{1,a,a^2,\cdots,a^{k-1}\}$，则 $|H|=k$. 只需证明 $H=\langle a\rangle$. 显然 $H\subseteq\langle a\rangle$. 关于反包含，取 $a^i\in\langle a\rangle$，由带余除法，$i=kq+r$，其中 $0\leqslant r<k$，因此 $a^i=a^{qk+r}=a^{qk}a^r=(a^k)^qa^r=a^r\in H$，由此可得 $\langle a\rangle\subseteq H$，从而 $\langle a\rangle=H$. ■

定义 如果 G 是有限群，则 G 中元素的个数称为 G 的**阶**，记为 $|G|$.

阶这个词有两个意义，即元素 $a\in G$ 的阶和群 G 的阶. 命题 2.34 证明群元素 a 的阶等于 $|\langle a\rangle|$.

命题 2.35 群 G 的任一子群族的交 $\bigcap_{i\in I}H_i$ 也是 G 的子群. 特别地，如果 H 和 K 都是 G 的子群，则 $H\cap K$ 也是 G 的子群.

证明概要 容易从定义得到. ■

系 2.36 如果 X 是群 G 的子集，则存在包含 X 的 G 的**最小子群** $\langle X\rangle$，最小是指对于 G 的每个包含 X 的子群 H 有 $\langle X\rangle\leqslant H$.

证明 G 的包含 X 的子群是存在的，如 G 本身就包含 X. 定义 $\langle X\rangle=\bigcap_{X\subseteq H}H$，$G$ 的一切包含 X 的子群的交. 根据命题 2.35，$\langle X\rangle$ 是 G 的子群，因为每个 H 包含 X，自然 $\langle X\rangle$ 包含 X. 最后，如果 H 是包含 X 的任一子群，则 H 是交成 $\langle X\rangle$ 的子群中的一个，即 $\langle X\rangle\leqslant H$. ■

注意上面的系中对子集 X 没有任何限制，特别是可允许 $X=\varnothing$. 因为空集是每个集合的子集，所以对每个 G 的子群 H 都有 $\varnothing\subseteq H$，于是 $\langle\varnothing\rangle$ 是 G 的一切子群的交，特别是有 $\langle\varnothing\rangle\leqslant\{1\}$，从而 $\langle\varnothing\rangle=\{1\}$.

定义 如果 X 是群 G 的子集，则称 $\langle X\rangle$ 为由 X **生成的子群**.

如果 X 是群 G 的非空子集，定义 X 上的**字**[⊖] 为形如 $g=x_1^{e_1}\cdots x_n^{e_n}$ 的元素 $g\in G$，其中对一切 i，$x_i\in X, e_i=\pm 1$.

66

命题 2.37 如果 X 是群 G 的非空子集，则 $\langle X\rangle$ 是 X 上所有字的集合.

⊖ 讨论自由群时这个定义要稍作修改.

证明 我们断言 X 上所有字的集合 $W(X)$ 是子群. 如果 $x \in X$，则 $1 = xx^{-1} \in W(X)$，X 上两个字的积也是 X 上的字，X 上的字的逆也是 X 上的字. 显然有 $X \subseteq W(X)$，所以 $\langle X \rangle \leqslant W(X)$（$\langle X \rangle$ 是 G 的包含 X 的一切子群的交）. 另一方面，G 的包含 X 的任一子群必包含 $W(X)$，从而 $\langle X \rangle = W(X)$. ■

例 2.38 （ⅰ）如果 $G = \langle a \rangle$ 是具有生成元 a 的循环群，则 G 由子集 $X = \{a\}$ 生成.

（ⅱ）二面体群 D_{2n}（即正 n 边形的对称群）由 ρ 和 σ 生成，其中 ρ 是旋转 $(360/n)°$，σ 是一个反射. 注意这两个生成元满足等式 $\rho^n = 1, \sigma^2 = 1$ 和 $\sigma\rho\sigma = \rho^{-1}$. ■

或许关于有限群 G 的子群 H 的最基本的事实是它们的阶有约束. 当然 $|H| \leqslant |G|$，其实 $|H|$ 还必定是 $|G|$ 的因数. 为证明这一事实，我们引入陪集的概念.

定义 如果 H 是群 G 的子群且 $a \in G$，则 G 的子集 aH 叫做**陪集** aH，其中

$$aH = \{ah : h \in H\}.$$

这里所定义的陪集常称为**左陪集**，还有 H 的**右陪集**，就是形如 $Ha = \{ha : h \in H\}$ 的子集. 将会看到左陪集和右陪集一般是不同的.

如果群 G 的运算使用记号 $*$，则记陪集 aH 为 $a * H$，其中

$$a * H = \{a * h : h \in H\}.$$

特别地，如果运算是加法，则陪集记为

$$a + H = \{a + h : h \in H\}.$$

当然，$a = a1 \in aH$. 通常，陪集不是子群，例如，如果 $a \notin H$，则 $1 \notin aH$（否则有某个 $h \in H$ 使得 $1 = ah$，从而与 $a = h^{-1} \in H$ 产生矛盾）.

例 2.39 （ⅰ）考虑作为（加法）阿贝尔群的平面 $\mathbb{R}^2$. 设 L 是通过原点 O 的直线（见图 2.7），如例2.29（ⅱ），直线 L 是 $\mathbb{R}^2$ 的子群. 如果 $\beta \in \mathbb{R}^2$，则陪集 $\beta + L$ 是包含 β 平行于 L 的直线 L'，这是因为如果 $r\alpha \in L$，则由平行四边形法则，$\beta + r\alpha \in L'$.

67

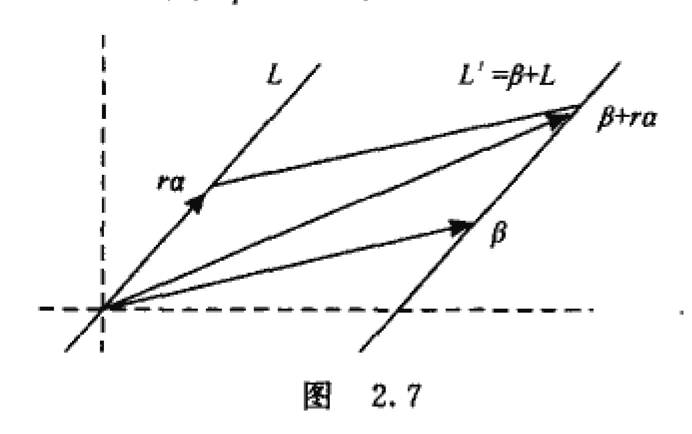


图 2.7

（ⅱ）设 A 是 $m \times n$ 实数矩阵，并设 $A\boldsymbol{x} = \boldsymbol{b}$ 是相容的线性方程组；即存在列向量 $\boldsymbol{s} \in \mathbb{R}^n$ 使得 $A\boldsymbol{s} = \boldsymbol{b}$. 齐次方程组 $A\boldsymbol{x} = \boldsymbol{0}$ 的**解空间** $S = \{\boldsymbol{x} \in \mathbb{R}^n : A\boldsymbol{x} = \boldsymbol{0}\}$ 是 $\mathbb{R}^n$ 的加法子群，原来的非齐次方程组的**解集** $\{\boldsymbol{x} \in \mathbb{R}^n : A\boldsymbol{x} = \boldsymbol{b}\}$ 是陪集 $\boldsymbol{s} + S$.

（ⅲ）如果 $G = S_3$ 且 $H = \langle(1\ 2)\rangle$，则 H 恰有三个左陪集，就是

$$H = \{(1), (1\ 2)\} = (1\ 2)H,$$
$$(1\ 3)H = \{(1\ 3), (1\ 2\ 3)\} = (1\ 2\ 3)H,$$
$$(2\ 3)H = \{(2\ 3), (1\ 3\ 2)\} = (1\ 3\ 2)H,$$

每一个的大小都是 2. 注意这些陪集也是“平行的”；即不同陪集不相交.

考虑 S_3 中 $H = \langle(1\ 2)\rangle$ 的右陪集：

$$H = \{(1),(1\ 2)\} = H(1\ 2),$$
$$H(1\ 3)= \{(1\ 3),(1\ 3\ 2)\} = H(1\ 3\ 2),$$
$$H(2\ 3)= \{(2\ 3),(1\ 2\ 3)\} = H(1\ 2\ 3).$$

再次看到恰有三个(右)陪集，每个大小为2. 注意这些陪集也是"平行的"；即不同(右)陪集不相交. ■

引理 2.40 设 H 是群 G 的子群，并设 $a,b \in G$.

(i) $aH = bH$ 当且仅当 $b^{-1}a \in H$. 特别地，$aH = H$ 当且仅当 $a \in H$.

(ii) 如果 $aH \cap bH \neq \varnothing$，则 $aH = bH$.

(iii) 对一切 $a \in G$, $|aH| = |H|$.

68

注 习题 2.29 证明 $Ha = Hb$ 当且仅当 $ab^{-1} \in H$，因此 $Ha = H$ 当且仅当 $a \in H$.

证明概要 对于前两个陈述，考虑 G 上如下定义的关系：$a \equiv b$ 如果 $b^{-1}a \in H$. 这是一个等价关系，它的等价类就是陪集. 由命题 1.54，H 的陪集划分 G. 第三个陈述为真是因为 $h \mapsto ah$ 是 $H \to aH$ 的双射. ■

下一定理以拉格朗日的名字命名，1770 年他知道 S_n 的某种子群的阶是 $n!$ 的因数. 群的概念是 60 年之后伽罗瓦发现的，有可能伽罗瓦是第一个圆满证明该定理的人.

定理 2.41(拉格朗日定理) 如果 H 是有限群 G 的子群，则 $|H|$ 是 $|G|$ 的因数.

证明 设 $\{a_1H, a_2H, \cdots, a_tH\}$ 是 G 中一切不同陪集的族，则

$$G = a_1H \cup a_2H \cup \cdots \cup a_tH.$$

这是因为每个 $g \in G$ 在陪集 gH 之内，且有某个 i 使得 $gH = a_iH$. 并且引理2.40(ii)又证明了陪集把 G 划分为两两不相交的子集，因此

$$|G| = |a_1H| + |a_2H| + \cdots + |a_tH|.$$

而由引理2.40(iii)，对一切 i 有 $|a_iH| = |H|$，所以正如所要求的那样 $|G| = t|H|$. ■

定义 G 中子群 H 的**指数**是指 G 中 H 的左[㊀]陪集的个数，记为 $[G:H]$.

指数 $[G:H]$ 就是证明拉格朗日定理时公式 $|G| = t|H|$ 中的数 t，因此

$$|G| = [G:H]|H|;$$

该公式说明指数 $[G:H]$ 也是 $|G|$ 的因数，且

$$[G:H] = |G|/|H|.$$

例 2.42 回忆二面体群 $D_{2n} = \Sigma(\pi_n)$，即正 n 边形 π_n 的对称群，它的阶为 $2n$ 并有一个由旋转 ρ 生成的 n 阶子群. 子群 $\langle\rho\rangle$ 有指数 $[D_{2n}:\langle\rho\rangle] = 2$，因此有两个陪集：$\langle\rho\rangle$ 和 $\sigma\langle\rho\rangle$，其中 σ 是 $\langle\rho\rangle$ 之外的任一反射，从而每个元素 $\alpha \in D_{2n}$ 都有因子分解 $\alpha = \sigma^i\rho^j$，其中 $i = 0,1$ 且 $0 \leqslant j < n$. ■

69

系 2.43 设 G 是有限群，$a \in G$，则 a 的阶是 $|G|$ 的因数.

证明 从命题 2.34 立即可以得证，因为 a 的阶是 $|\langle a\rangle|$. ■

系 2.44 如果 G 是有限群，则对一切 $a \in G$, $a^{|G|} = 1$.

证明 如果 a 的阶是 d，则由上一个系，存在某个整数 m 使得 $|G| = dm$，从而 $a^{|G|} = a^{dm} = (a^d)^m = 1$. ■

系 2.45 如果 p 是素数，则每个阶为 p 的群 G 都是循环群.

㊀ 习题 2.37 证明一个子群的左陪集的个数等于它的右陪集的个数.

证明　如果 $a \in G$ 且 $a \neq 1$，则 a 的阶 $d > 1$ 且 d 是 p 的因数，因为 p 是素数，$d = p$，所以 $G = \langle a \rangle$. ■

我们已经知道$\mathbb{I}_m$ 在加法下是 m 阶循环群，现在由

$$[a][b] = [ab]$$

给出乘法 $\mu: \mathbb{I}_m \times \mathbb{I}_m \to \mathbb{I}_m$，它也是$\mathbb{I}_m$ 上的二元运算（由命题1.20，它是合理定义的），并且是结合的、交换的，[1] 是幺元. 但$\mathbb{I}_m$ 在这个运算下不是群，因为其逆可能不存在，例如 [0] 就没有乘法逆.

命题 2.46　*定义集合 $U(\mathbb{I}_m)$ 为*

$$U(\mathbb{I}_m) = \{[r] \in \mathbb{I}_m : (r,m) = 1\},$$

它是阶为 $\phi(m)$ 的乘法群，其中 ϕ 是欧拉 ϕ－函数. 特别地，如果 p 是素数，则 $U(\mathbb{I}_p) = \mathbb{I}_p^\times$ 是阶为 $p-1$ 的乘法群，其中 $\mathbb{I}_p^\times$ 是 $\mathbb{I}_p$ 的非零元素的集合.

证明　由习题1.14，$(r,m) = 1 = (r',m)$ 蕴涵 $(rr',m) = 1$，因此 $U(\mathbb{I}_m)$ 在乘法下封闭. 前面已经提到该乘法是结合的，[1] 是幺元. 如果 $(a,m) = 1$，则在$\mathbb{I}_m$ 中可关于 $[x]$ 求解 $[a][x] = [1]$. 现在 $(x,m) = 1$，这是因为存在某个整数 s 使得 $ra + sm = 1$，由命题1.13可得 $(x,m) = 1$，所以 $[x] \in U(\mathbb{I}_m)$，由此每个 $[r] \in U(\mathbb{I}_m)$ 都有逆，因此 $U(\mathbb{I}_m)$ 是群. 欧拉 ϕ－函数的定义表明 $|U(\mathbb{I}_m)| = \phi(m)$.

当 p 是素数时，$\phi(p) = p - 1$，由此得最后一个陈述. ■

第3章中将证明对每个素数 p，$\mathbb{I}_p^\times$ 是循环群.

下面是费马定理，即定理1.24的群论证明，原先的证明用到了二项式系数和 $p \mid \binom{p}{r} (0 < r < p)$ 的事实.

系 2.47（费马）　*如果 p 是素数，$a \in \mathbb{Z}$，则*

70

$$a^p \equiv a \bmod p.$$

证明　只需证明在 $\mathbb{I}_p$ 中$[a^p] = [a]$. 如果 $[a] = [0]$，则 $[a^p] = [a]^p = [0]^p = [0] = [a]$. 如果 $[a] \neq [0]$，则$[a] \in \mathbb{I}_p^\times$，它是 $\mathbb{I}_p$ 中非零元素的乘法群. 因 $|\mathbb{I}_p^\times| = p-1$，由拉格朗日定理的系2.44，$[a]^{p-1} = [1]$. 乘 $[a]$ 可得要求证明的结果 $[a^p] = [a]^p = [a]$. 所以 $a^p \equiv a \bmod p$. ■

现在给出欧拉对费马定理的推广.

定理 2.48（欧拉）　*如果 $(r,m) = 1$，则*

$$r^{\phi(m)} \equiv 1 \bmod m.$$

证明　因 $|U(\mathbb{I}_m)| = \phi(m)$，系2.44（本质上是拉格朗日定理）给出：对一切 $[r] \in U(\mathbb{I}_m)$，$[r]^{\phi(m)} = [1]$. 用同余记号是：如果 $(r,m) = 1$，则 $r^{\phi(m)} \equiv 1 \bmod m$. ■

例 2.49　易知

$$U(\mathbb{I}_8) = \{[1],[3],[5],[7]\}$$

是群（类似四群 V），其每个元素的平方是 [1]，而

$$U(\mathbb{I}_{10}) = \{[1],[3],[7],[9]\}$$

是4阶的循环群 [下一节引入同构后，称 $U(\mathbb{I}_8)$ 与 $\mathbf{V}$ 同构，而 $U(\mathbb{I}_{10})$ 与$\mathbb{I}_4$ 同构]. ■

定理 2.50（威尔逊定理）　*整数 p 是素数当且仅当*

$$(p-1)! \equiv -1 \bmod p.$$

证明 假定 p 是素数. 如果 $a_1,a_2,\cdots,a_n$ 是一个有限阿贝尔群的所有元素的表，则乘积 $a_1a_2\cdots a_n$ 与满足 $a^2=1$ 的所有元素的乘积是一样的，这是因为任一其他元素和它的逆互相抵消. 因 p 是素数，习题 1.37 蕴涵 $\mathbb{I}_p^\times$ 只有一个 2 阶元素，即 $[-1]$，由此，$\mathbb{I}_p^\times$ 中所有元素的乘积（即 $[(p-1)!]$）等于 $[-1]$，所以 $(p-1)!\equiv -1 \bmod p$.

反之，假定 m 是合数：存在整数 a 和 b 使得 $m=ab$ 且 $1<a\leqslant b<m$. 如果 $a<b$，则 $m=ab$ 是 $(m-1)!$ 的因数，因此 $(m-1)!\equiv 0 \bmod m$. 如果 $a=b$，则 $m=a^2$. 如果 $a=2$，则 $(a^2-1)!=3!=6\equiv 2 \bmod 4$，自然 $2\not\equiv -1 \bmod 4$. 如果 $2<a$，则 $2a<a^2$，因此 a 和 $2a$ 是 $(a^2-1)!$ 的因数，所以 $(a^2-1)!\equiv 0 \bmod a^2$，从而 $(a^2-1)!\not\equiv -1 \bmod a^2$. 证明完成. ■ [71]

注 可以像欧拉定理推广费马定理那样推广威尔逊（Wilson）定理：用 $U(\mathbb{I}_m)$ 替换 $U(\mathbb{I}_p)$. 例如，对一切 $m\geqslant 3$，可以证明 $U(\mathbb{I}_{2^m})$ 恰有三个 2 阶元素，即 $[-1],[1+2^{m-1}]$ 和 $[-(1+2^{m-1})]$. 现在可导出满足 $1\leqslant r<2^m$ 的一切奇数 r 的乘积和 1 对于 mod 2^m 同余，因为

$$(-1)(1+2^{m-1})(-1-2^{m-1})=(1+2^{m-1})^2$$
$$=1+2^m+2^{2m-2}\equiv 1 \bmod 2^m.$$

习题

2.29 设 H 是群 G 的子群.

（i）证明右陪集 Ha 和 Hb 相等当且仅当 $ab^{-1}\in H$.

（ii）证明：关系 $a\equiv b$ 如果 $ab^{-1}\in H$ 是 G 上的等价关系，它的等价类是 H 的右陪集.

2.30 （i）定义**特殊线性群**为

$$\mathrm{SL}(2,\mathbb{R})=\{A\in \mathrm{GL}(2,\mathbb{R}): \det(A)=1\}.$$

证明 $\mathrm{SL}(2,\mathbb{R})$ 是 $\mathrm{GL}(2,\mathbb{R})$ 的子群.

（ii）证明 $\mathrm{GL}(2,\mathbb{Q})$ 是 $\mathrm{GL}(2,\mathbb{R})$ 的子群.

2.31 （i）举出一个群 G 的两个子群 H 和 K 的例子，其并 $H\cup K$ 不是 G 的子群.

提示：设 G 是四群 **V**.

（ii）证明两个子群的并 $H\cup K$ 其本身是子群当且仅当 H 是 K 的子集或 K 是 H 的子集.

2.32 设有限群 G 有子群 H 和 K. 如果 $H\leqslant K$，证明

$$[G:H]=[G:K][K:H].$$

2.33 如果 H 和 K 是群 G 的子群，且 $|H|$ 和 $|K|$ 互素，证明 $H\cap K=\{1\}$.

提示：如果 $x\in H\cap K$，则 $x^{|H|}=1=x^{|K|}$.

2.34 证明循环群 $G=\langle a\rangle$ 的每个子群 S 本身也是循环群.

提示：如果 $S\neq 1$，选取 k 为满足 $a^k\in S$ 的最小正整数.

2.35 设 G 是 n 阶的循环群，证明对每个整除 n 的 d，G 有 d 阶子群.

提示：如果 $G=\langle a\rangle$ 且 $n=dk$，考虑 $\langle a^k\rangle$.

2.36 设 G 是 4 阶群，证明 G 要么是循环群，要么对每个 $x\in G$ 有 $x^2=1$. 由此，根据习题 2.26 可知，G 必是阿贝尔群.

2.37 如果 H 是群 G 的子群，证明 G 中 H 的左陪集的个数和 G 中 H 的右陪集的个数相等.

提示：函数 $\varphi: aH\mapsto Ha^{-1}$ 是从 H 的全部左陪集族到 H 的全部右陪集族的双射. [72]

2.38 设 p 是奇素数且 $a_1,\cdots,a_{p-1}$ 是 $\{1,2,\cdots,p-1\}$ 的一个置换. 证明存在 $i\neq j$ 使得 $ia_i\equiv ja_j \bmod p$.

提示：用威尔逊定理.

2.5 同态

一个重要问题是确定给出的两个群 G 和 H 是否有某种共性．例如，我们已经研究过 S_3，即 $X=\{1,2,3\}$ 的全体置换组成的群．$Y=\{a,b,c\}$ 的全体置换组成的群 S_Y 与 S_3 不同，因为$\{1,2,3\}$的置换与$\{a,b,c\}$的置换不同．尽管 S_Y 与 S_3 不同，但它们彼此确实很相像(见例 2.51)．更有趣的例子是 S_3 和等边三角形的对称群 D_6 也很相像．我们将看到同态和同构的概念可用来比较不同的群．

定义 如果 $(G,*)$，$(H,\circ)$ 是群(两个群的运算已表示出来)，则函数 $f:G\to H$ 称为**同态**[⊖]，如果对一切 $x,y\in G$，

$$f(x*y)=f(x)\circ f(y).$$

如果 f 还是一个双射，则称 f 为**同构**．两个群 G 和 H 称为**同构的**，如果它们之间存在同构 $f:G\to H$，记为 $G\cong H$．

群 G 的乘法表是把每个乘积 ab（其中 $a,b\in G$）表示出来的表格．

G	a_1	a_2	$\cdots$	a_j	$\cdots$	a_n
a_1	a_1a_1	a_1a_2	$\cdots$	a_1a_j	$\cdots$	a_1a_n
a_2	a_2a_1	a_2a_2	$\cdots$	a_2a_j	$\cdots$	a_2a_n
a_i	a_ia_1	a_ia_2	$\cdots$	a_ia_j	$\cdots$	a_ia_n
a_n	a_na_1	a_na_2	$\cdots$	a_na_j	$\cdots$	a_na_n

定义 设 $a_1,a_2,\cdots,a_n$ 是群 G 所有元素无重复的表，G 的**乘法表**是指一个 $n\times n$ 阵列，处于 ij 位置是元素 a_ia_j．

73

n 阶群 G 的乘法表依赖于如何排列 G 的元素，从而 G 有 $n!$ 个不同的乘法表(由此，判定一个群 G 的乘法表是否和另一个群 H 的乘法表相同是一项骇人的任务：需要比较 $n!$ 张表，每张表又要比较 n^2 个元素)．如果 $a_1,a_2,\cdots,a_n$ 是群 G 所有元素无重复的表，且 $f:G\to H$ 是双射，则 $f(a_1)$，$f(a_2),\cdots,f(a_n)$ 是 H 所有元素无重复的表，这个表可以确定 H 的一个乘法表．f 是同构的意思是说，如果把给定的 G 的（由 $a_1,a_2,\cdots,a_n$ 确定的)乘法表重叠到 H 的(由 $f(a_1),f(a_2),\cdots,f(a_n)$ 确定的)乘法表上，则两个表相匹配：如果 a_ia_j 是给定的 G 的乘法表中处于 ij 位置的元素，则 $f(a_i)f(a_j)=f(a_ia_j)$ 是 H 的乘法表中处于 ij 位置的元素．在此意义下，同构群有相同的乘法表，于是同构群本质上是相同的，不同的只是元素和运算的记号．

例 2.51 我们来证明置换 $\{1,2,3\}$ 的对称群 $G=S_3$ 和 $Y=\{a,b,c\}$ 的全体置换组成的对称群 $H=S_Y$ 同构．首先列举 G 的元素：

$$(1),(1\ 2),(1\ 3),(2\ 3),(1\ 2\ 3),(1\ 3\ 2).$$

定义 $\varphi:S_3\to S_Y$ 为明显的用字母替换数字的函数：

$$(1),(a\ b),(a\ c),(b\ c),(a\ b\ c),(a\ c\ b).$$

比较由 S_3 的元素表产生的乘法表和由 S_Y 的相应元素表产生的乘法表，读者需要写出两者的完整表格，并把一个表格放在另一个之上以检查匹配情况．这里只检查一个位置．S_3 的乘法表中处于 4，5

⊖ 词 homomorphism（同态）来自意为“相同”的希腊语 homo 和意为“形状”或“形式”的希腊语 morph．这样，同态把一个群带到有相似形式的另一个群（它的象）．词 isomorphism（同构）与意为“相等”的希腊语 iso 有关．同构群有相同的形式．

位置的是乘积 $(2\ 3)(1\ 2\ 3) = (1\ 3)$，而 S_Y 的乘法表中处于 4，5 位置的是 $(b\ c)(a\ b\ c) = (a\ c)$.

习题 2.39 推广了这个结果. ■

引理 2.52 设 $f: G \to H$ 是群同态.

(ⅰ) $f(1) = 1$.

(ⅱ) $f(x^{-1}) = f(x)^{-1}$.

(ⅲ) 对一切 $n \in \mathbb{Z}$，$f(x^n) = f(x)^n$.

证明概要 (ⅰ) $1 \cdot 1 = 1$ 蕴涵 $f(1)f(1) = f(1)$.

(ⅱ) $1 = xx^{-1}$ 蕴涵 $1 = f(1) = f(x)f(x^{-1})$.

(ⅲ) 对一切 $n \geqslant 0$ 用归纳法证明 $f(x^n) = f(x)^n$. 注意到 $x^{-n} = (x^{-1})^n$，再用 (ⅱ). ■ 74

例 2.53 如果 H 和 G 都是 m 阶循环群，则 H 和 G 同构(由此，根据系 2.45，阶为素数 p 的任两个群都同构). 证明虽不难，但需要小心. 我们有 $G = \{1, a, a^2, \cdots, a^{m-1}\}$，$H = \{1, b, b^2, \cdots, b^{m-1}\}$，对于同构的明显选择是令双射 $f: G \to H$ 为 $f(a^i) = b^i$. 验证 f 是同构就是验证 $f(a^i a^j) = b^{i+j}$，这要牵涉到两种情形：$i + j \leqslant m - 1$ 和 $i + j > m - 1$. 例 2.71 给出了一个计算量较少的证明. ■

群 G 的一个性质为任一同构于它的群所共有称为 G 的一个**不变量**. 例如阶 $|G|$ 就是 G 的一个不变量，这是因为同构群有相同的阶. 阿贝尔群也是一个不变量 [如果 f 是同构且 a 和 b 可交换，则 $ab = ba$ 且

$$f(a)f(b) = f(ab) = f(ba) = f(b)f(a);$$

因此 $f(a)$ 和 $f(b)$ 可交换]. 由此 $\mathbb{I}_6$ 和 S_3 不同构，因为 $\mathbb{I}_6$ 是阿贝尔群而 S_3 不是. 一般来说，判定两个给定的群是否同构是一个具有挑战性的问题. 更多不变量的例子见习题 2.42.

例 2.54 我们举出两个有相同的阶但不同构的阿贝尔群.

如例2.29(ⅰ)，设 $\mathbf{V}$ 是四群，它由下列四个置换组成：

$$\mathbf{V} = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\},$$

设 $\mu_4 = \langle \mathrm{i} \rangle = \{1, \mathrm{i}, -1, -\mathrm{i}\}$ 是 4 次单位根的乘法循环群，其中 $\mathrm{i}^2 = -1$. 如果有同构 $f: \mathbf{V} \to \mu_4$，则因 f 是满射，将有 $x \in \mathbf{V}$ 满足 $\mathrm{i} = f(x)$. 但对一切 $x \in \mathbf{V}$，$x^2 = (1)$，因此 $\mathrm{i}^2 = f(x)^2 = f(x^2) = f((1)) = 1$，与 $\mathrm{i}^2 = -1$ 矛盾. 所以 $\mathbf{V}$ 和 μ_4 不同构.

有其他方法证明该结果. 例如 μ_4 是循环群而 $\mathbf{V}$ 不是；μ_4 有 4 阶元素而 $\mathbf{V}$ 没有；μ_4 中 2 阶元素是唯一的，而 $\mathbf{V}$ 有三个 2 阶元素. 到此该确信 $\mathbf{V}$ 和 μ_4 不同构吧！ ■

定义 设 $f: G \to H$ 是同态，定义

$$f \text{ 的核}^{\ominus} = \{x \in G : f(x) = 1\}$$

和

$$f \text{ 的象} = \{h \in H : \text{存在某个 } x \in G \text{ 使得 } h = f(x)\}.$$

通常记 f 的核为 $\ker f$，f 的象为 $\operatorname{im} f$. 75

例 2.55 (ⅰ) 如果 μ_2 是乘法群 $\mu_2 = \{\pm 1\}$，则由定理 2.12，$\mathrm{sgn}: S_n \to \mu_2$ 是同态，sgn 的核是交错群 A_n，它是一切偶置换的集合.

(ⅱ) 行列式是满同态 $\det: \mathrm{GL}(n, \mathbb{R}) \to \mathbb{R}^{\times}$，$\mathbb{R}^{\times}$ 是非零实数的乘法群，其核是一切行列式为 1 的 $n \times n$ 矩阵的特殊线性群 $\mathrm{SL}(n, \mathbb{R})$. ■

⊖ kernel（核）来自意为“谷物”或“种子”的德语字（corn 也来自同一字），用在这里是指同态的一个重要成分.

命题 2.56 设 $f: G \to H$ 是同态.

(i) $\ker f$ 是 G 的子群，$\operatorname{im} f$ 是 H 的子群.

(ii) 如果 $x \in \ker f, a \in G$，则 $axa^{-1} \in \ker f$.

(iii) f 是单射当且仅当 $\ker f = \{1\}$.

证明概要 (i) 显然成立.

(ii) $f(axa^{-1}) = f(a)1f(a)^{-1} = 1$.

(iii) $f(a) = f(b)$ 当且仅当 $f(b^{-1}a) = 1$. ■

定义 群 G 的子群 K 称为**正规子群**，如果 $k \in K$ 和 $g \in G$ 蕴涵 $gkg^{-1} \in K$. 如果 K 是 G 的正规子群，记为 $K \lhd G$.

上一命题说同态的核恒为正规子群. 如果 G 是阿贝尔群，则每个子群 K 都是正规子群，这是因为如果 $k \in K, g \in G$，则 $gkg^{-1} = kgg^{-1} = k \in K$. 这个陈述的逆不成立：在例 2.63 中将看到，有一个非阿贝尔群(四元数群)，它的每个子群都是正规子群.

S_3 的循环子群 $H = \langle (1\ 2) \rangle$ 由两个元素 (1) 和 (1 2) 组成，它不是 S_3 的正规子群：如果 $\alpha = (1\ 2\ 3)$，则 $\alpha^{-1} = (3\ 2\ 1)$，而

$$\alpha(1\ 2)\alpha^{-1} = (1\ 2\ 3)(1\ 2)(3\ 2\ 1) = (2\ 3) \notin H$$

[由定理 2.9，$\alpha(1\ 2)\alpha^{-1} = (\alpha 1\ \alpha 2) = (2\ 3)$]. 另一方面，$S_3$ 的循环子群 $K = \langle (1\ 2\ 3) \rangle$ 是正规子群，读者可以自行验证.

由例 2.55(i) 和 2.55(ii) 可知 A_n 是 S_n 的正规子群，$\mathrm{SL}(n, \mathbb{R})$ 是 $\mathrm{GL}(n, \mathbb{R})$ 的正规子群(不过也容易直接证明).

定义 如果 G 是群，$a \in G$，则形如

$$gag^{-1}$$

的 G 中的任一元素称为 a 的一个**共轭元素**，其中 $g \in G$.

显然，子群 $K \leqslant G$ 是正规子群当且仅当 K 包含它的元素的一切共轭元素：如果 $k \in K$，则对一切 $g \in G, gkg^{-1} \in K$.

76

例 2.57 (i) 定理 2.9 叙述了 S_n 中两个置换共轭当且仅当它们有相同的轮换结构.

(ii) 在线性代数中，把两个矩阵 $A, B \in \mathrm{GL}(n, \mathbb{R})$ 共轭称为**相似**，即存在非奇异矩阵 P 使得 $B = PAP^{-1}$. ■

定义 如果 G 是群，$g \in G$，定义**共轭** $\gamma_g: G \to G$ 为对一切 $a \in G$，

$$\gamma_g(a) = gag^{-1}.$$

命题 2.58 (i) 设 G 是群，$g \in G$，则共轭 $\gamma_g: G \to G$ 是同构.

(ii) 共轭元素有相同的阶.

证明 (i) 如果 $g, h \in G$，则

$$(\gamma_g \circ \gamma_h)(a) = \gamma_g(hah^{-1}) = g(hah^{-1})g^{-1} = (gh)a(gh)^{-1} = \gamma_{gh}(a);$$

即

$$\gamma_g \circ \gamma_h = \gamma_{gh}.$$

由此 $\gamma_g \circ \gamma_{g^{-1}} = \gamma_1 = 1 = \gamma_{g^{-1}} \circ \gamma_g$，所以 γ_g 是双射. 现在证明 γ_g 是同构：如果 $a, b \in G$，则

$$\gamma_g(ab) = g(ab)g^{-1} = ga(g^{-1}g)bg^{-1} = \gamma_g(a)\gamma_g(b).$$

(ii) 称 a，b 共轭就是指存在 $g \in G$ 使得 $b = gag^{-1}$，也就是 $b = \gamma_g(a)$，而 γ_g 是同构，习题

2.42 证明 a 和 $b=\gamma_g(a)$ 有相同的阶. ■

例 2.59　群 G 的**中心**，记为 $Z(G)$，定义为

$$Z(G)=\{z\in G:\text{对一切 } g\in G, zg=gz\},$$

即 $Z(G)$ 由能和 G 中每个元素交换的一切元素组成.

易知 $Z(G)$ 是 G 的子群，它还是正规子群，因为如果 $z\in Z(G), g\in G$，则

$$gzg^{-1}=zgg^{-1}=z\in Z(G).$$

群 G 是阿贝尔群当且仅当 $Z(G)=G$. 另一极端是 $Z(G)=\{1\}$，这样的群 G 叫做**无中心群**. 例如 $Z(S_3)=\{1\}$，其实所有大的对称群都是无中心的，习题 2.15 证明对一切 $n\geqslant 3, Z(S_n)=\{1\}$. ■

[77]

例 2.60　如果 G 是群，则同构 $f:G\to G$ 称为 G 的**自同构**. 例如每个共轭 γ_g 就是 G 的自同构（称为**内自同构**），因为它的逆是 g^{-1} 形成的共轭. G 的一切自同构的集合 $\mathrm{Aut}(G)$ 在复合下也是一个群，而一切共轭的集合

$$\mathrm{Inn}(G)=\{\gamma_g : g\in G\}$$

是 $\mathrm{Aut}(G)$ 的子群. 习题 2.64 说由 $g\mapsto\gamma_g$ 给出的函数 $\Gamma:G\to\mathrm{Aut}(G)$ 是同态，且有 $\mathrm{im}\Gamma=\mathrm{Inn}(G)$，$\ker\Gamma=Z(G)$；此外 $\mathrm{Inn}(G)\lhd\mathrm{Aut}(G)$. ■

例 2.61　四群 $\mathbf{V}$ 是 S_4 的正规子群. 回忆 $\mathbf{V}$ 的元素是

$$\mathbf{V}=\{(1),(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}.$$

由定理 2.9，两个对换之积的共轭也是两个对换的积，而在例2.5(ⅰ)中已知 S_4 仅有 3 个置换有这样的轮换结构，所以 $\mathbf{V}$ 是 S_4 的正规子群. ■

命题 2.62　（ⅰ）*如果 H 是群 G 中指数为 2 的子群，则对每个 $g\in G, g^2\in H$.*

（ⅱ）*如果 H 是群 G 中指数为 2 的子群，则 H 是 G 的正规子群.*

证明　（ⅰ）因为 H 的指数为 2，它恰有两个陪集，就是 H 和 aH，其中 $a\notin H$，于是 G 是不相交并 $G=H\uplus aH$. 取 $g\in G$ 且 $g\notin H$，则有 $h\in H$ 使得 $g=ah$. 如果 $g^2\notin H$，则 $g^2=ah'$，其中 $h'\in H$，因此

$$g=g^{-1}g^2=h^{-1}a^{-1}ah'=h^{-1}h'\in H,$$

这是一个矛盾.

（ⅱ）[一]只需证明：如果 $h\in H$，则对每个 $g\in G$，共轭 $ghg^{-1}\in H$. 因 H 的指数为 2，H 恰有两个陪集，就是 H 和 aH，其中 $a\notin H$，因此 $g\in H$ 或 $g\in aH$. 如果 $g\in H$，则因 H 是子群，$ghg^{-1}\in H$. 对第二种情形，可令 $g=ax$，其中 $x\in H$，于是 $ghg^{-1}=a(xhx^{-1})a^{-1}=ah'a^{-1}$，其中 $h'=xhx^{-1}\in H$（因 h' 是 H 中三个元素的积）. 如果 $ghg^{-1}\notin H$，则 $ghg^{-1}=ah'a^{-1}\in aH$；即有某个 $y\in H$ 使得 $ah'a^{-1}=ay$. 消去 a 得 $h'a^{-1}=y$，这就出现矛盾 $a=y^{-1}h'\in H$. 所以，如果 $h\in H$，则它的每个共轭都在 H 中；即 H 是 G 的正规子群. ■

[78]

定义　$\mathrm{GL}(2,\mathbb{C})$ 中下列元素

$$\mathbf{Q}=\{I,A,A^2,A^3,B,BA,BA^2,BA^3\}$$

组成的 8 阶群 $\mathbf{Q}$ 称为**四元数群**[二]，其中 I 是单位矩阵，

㊀ 习题 2.50 给出另一个证明.

㊁ 哈密顿（W. R. Hamilton）发现一个有两种运算（加法和乘法）的系统，因为是四维的，所以称之为四元数. 四元数群由该系统中 8 个特殊的元素组成. 见习题 2.60.

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}.$$

元素 $A \in \mathbf{Q}$ 的阶为 4，因此$\langle A \rangle$是 4 阶子群，因而指数为 2；另一个陪集是 $B\langle A \rangle = \{B, BA, BA^2, BA^3\}$，由此，$\mathbf{Q}$ 中的每个元素都有一个形如 $B^i A^j$ 的表达式，其中 $i = 0, 1, j = 0,1,2,3$.

例 2.63 在习题 2.59 中，读者将验证 $\mathbf{Q}$ 是 8 阶非阿贝尔群，它恰有一个 2 阶元素，从而只有一个 2 阶子群，即$\langle -I \rangle$. 我们断言 $\mathbf{Q}$ 的每个子群都是正规子群. 拉格朗日定理说 $\mathbf{Q}$ 的每个子群的阶都是 8 的因数，所以子群的阶只可能是 1，2，4 或 8. 显然子群$\{I\}$ 和 8 阶子群(即 $\mathbf{Q}$ 自己)是正规子群. 由命题 2.62(ⅱ)，任何 4 阶子群必是正规子群，因为它的指数为 2. 最后，子群$\langle -I \rangle$是正规的，因为它就是中心 $Z(\mathbf{Q})$. ■

例 2.63 表明 $\mathbf{Q}$ 是一个像阿贝尔群那样每个子群都是正规子群的非阿贝尔群. 本质上只有这一个例子. 每个子群都正规的非阿贝尔有限群叫做**哈密顿群**. 每个哈密顿群形为 $\mathbf{Q} \times A$，其中 A 是一个没有 4 阶元素的阿贝尔群(直积的概念将在下一节引入). 这个结果的证明见 Robinson 所著的《A Course in the Theory of Groups》139 页.

拉格朗日定理说有限群 G 的子群的阶必是 $|G|$ 的因数，由此引出一个问题，即给定 $|G|$ 的一个因数 d，G 是否必包含一个 d 阶子群. 下一结果表明未必有这样的子群.

命题 2.64 *交错群 A_4 是没有 6 阶子群的 12 阶群.*

证明 首先，由习题 2.12，$|A_4| = 12$. 如果 A_4 包含一个 6 阶子群 H，则 H 的指数为 2，从而根据命题 2.62(ⅰ)，对每个 $\alpha \in A_4, \alpha^2 \in H$. 然而，如果 α 是 3-轮换，则 α 的阶为 3，因此 $\alpha = \alpha^4 = (\alpha^2)^2$，从而 H 包含每个 3-轮换. 这是一个矛盾，因为 A_4 中有 8 个 3-轮换. ■

79

习题

2.39 证明：如果存在双射 $f: X \to Y$ (即 X 和 Y 的元素个数相等)，则存在同构 $\varphi: S_X \to S_Y$.

提示：如果 $\alpha \in S_X$，定义 $\varphi(\alpha) = f \circ \alpha \circ f^{-1}$. 特别地，如果 $|X| = 3$，则如同例 2.51 那样，φ 把包含符号 1，2，3 的轮换变成包含符号 a，b，c 的轮换.

2.40 (ⅰ) 证明同态的复合也是同态.

(ⅱ) 证明同构的逆是同构.

(ⅲ) 证明两个群都和第三个群同构，则它们彼此同构.

(ⅳ) 证明在群的任一集合上，同构是一个等价关系.

2.41 证明群 G 是阿贝尔群当且仅当由 $f(a) = a^{-1}$ 给出的函数 $f: G \to G$ 是同态.

2.42 本题给出群 G 的一些不变量. 设 $f: G \to H$ 是同构.

(ⅰ) 证明：如果 $a \in G$ 的阶有限，则 $f(a)$ 的阶有限，如果 a 有有限阶 n，则 $f(a)$ 也有有限阶 n. 由此可知，如果 G 有阶为某个 n 的元素而 H 没有，则 $G \not\cong H$.

(ⅱ) 证明：如果 $G \cong H$，则对于 $|G|$ 的每个因数 d，G 和 H 拥有 d 阶元素的个数相等.

2.43 证明 A_4 和 D_{12} 是 12 阶不同构的群.

2.44 (ⅰ) 求 S_4 的一个子群 H 满足 $H \neq \mathbf{V}$ 且 $H \cong \mathbf{V}$.

(ⅱ) 证明 (ⅰ) 中的子群 H 不是正规子群.

2.45 证明每个 $|G| < 6$ 的群 G 都是阿贝尔群.

2.46 设 $G=\{f:\mathbb{R}\to\mathbb{R}: f(x)=ax+b$，其中 $a\neq 0\}$. 证明 G 在复合下是群，它同构于由一切形如 $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$ 的矩阵组成的 $GL(2,\mathbb{R})$ 的子群.

2.47 (i) 设 $f:G\to H$ 是同态且 $x\in G$ 的阶为 k，证明 $f(x)\in H$ 的阶 m 满足 $m\mid k$.

(ii) 设 $f:G\to H$ 是同态且 $(|G|,|H|)=1$，证明对一切 $x\in G, f(x)=1$.

2.48 (i) 证明

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}^k = \begin{bmatrix} \cos k\theta & -\sin k\theta \\ \sin k\theta & \cos k\theta \end{bmatrix}.$$

提示：对 $k\geqslant 1$ 用归纳法.

(ii) 证明由一切行列式为 1 的 2×2 正交矩阵组成的特殊正交群 $SO(2,\mathbb{R})$ 和圆群 S^1 同构.

提示：考虑 $\varphi:\begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}\mapsto(\cos\alpha,\ \sin\alpha)$.

2.49 设 G 是系数在 $\mathbb{Z}$ 中的一切关于 x 的多项式组成的加法群，又设 H 是一切正有理数的乘法群，证明 $G\cong H$.

提示：列出素数 $p_0=2, p_1=3, p_2=5,\cdots$，定义

$$\varphi(e_0+e_1x+e_2x^2+\cdots+e_nx^n)=p_0^{e_0}\cdots p_n^{e_n}.$$

80

2.50 (i) 证明：如果子群 H 满足对每个 $b\in G$ 有 $bH=Hb=[hb: b\in H]$，则 H 必是正规子群.

(ii) 用 (i) 给出命题2.62(ii)的第二个证明：如果 $H\leqslant G$ 的阶为 2，则 $H\lhd G$.

提示：如果 $a\notin H$，则 $aH=H'=Ha$，其中 H' 是 H 的补集.

2.51 (i) 设 $\alpha\in S_n$，证明 α 和 α^{-1} 共轭.

(ii) 举出一个群 G 的例子，它包含一个元素 x 满足 x 与 x^{-1} 不共轭.

2.52 证明群 G 的任一正规子群族的交仍是 G 的正规子群.

2.53 定义 $W=\langle(1\ 2)(3\ 4)\rangle$，即 W 是由 $(1\ 2)(3\ 4)$ 生成的 S_4 的循环子群，证明 W 是 $\mathbf{V}$ 的正规子群，但 W 不是 S_4 的正规子群. 由此可知正规子群是不传递的：$W\lhd\mathbf{V}$ 和 $\mathbf{V}\lhd G$ 不蕴涵 $W\lhd G$.

2.54 设 G 是用乘法写出的有限阿贝尔群. 证明：如果 $|G|$ 是奇数，则每个 $x\in G$ 有唯一的平方根，即存在唯一的 $g\in G$ 使得 $g^2=x$.

提示：证明平方是 $G\to G$ 的单射函数，再运用习题 1.58.

2.55 举出一个群 G 的例子，它有子群 $H\leqslant G$ 和元素 $g\in G$，满足 $[G:H]=3$ 且 $g^3\notin H$.

提示：取 $G=S_3, H=\langle(1\ 2)\rangle, g=(2\ 3)$.

2.56 证明 $GL(2,\mathbb{R})$ 的中心是一切**标量矩阵** aI 的集合，其中 $a\neq 0$.

提示：证明：如果 A 不是标量矩阵，则有某个非奇异矩阵与 A 不交换.（推广到 $n\times n$ 矩阵也成立.）

2.57 设 $\zeta=e^{2\pi i/n}$ 是 n 次单位原根，定义

$$A=\begin{bmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{bmatrix},\quad B=\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

(i) 证明 A 的阶为 n，B 的阶为 2.

(ii) 证明 $BAB=A^{-1}$.

(iii) 证明：形如 A^i 和 BA^i 的矩阵组成乘法子群 $G\leqslant GL(2,\mathbb{C})$，其中 $0\leqslant i<n$.

提示：考虑 A^iA^j，A^iBA^j，BA^iA^j 和 $(BA^i)(BA^j)$ 各种情形.

(iv) 证明 G 中每个矩阵都可唯一地表示为 B^iA^j 的形式，其中 $i=0,1, 0\leqslant j<n$. 由此推出 $|G|=2n$.

(v) 证明 $G\cong D_{2n}$.

提示：把 G 中元素表示为 B^iA^j 的唯一表达式可用来定义函数 $G\to D_{2n}$.

2.58 (ⅰ) 证明 $\mathbf{Q}\times\mathbb{I}_2$ 的每个子群都是正规子群.

(ⅱ) 证明 $\mathbf{Q}\times\mathbb{I}_4$ 中存在非正规子群.

2.59 回忆四元数群 $\mathbf{Q}$ 由 $\mathrm{GL}(2,\mathbb{C})$ 中的 8 个矩阵组成，

81

$$\mathbf{Q}=\{I,A,A^2,A^3,B,BA,BA^2,BA^3\},$$

其中

$$A=\begin{bmatrix}0&1\\-1&0\end{bmatrix},\qquad B=\begin{bmatrix}0&\mathrm{i}\\\mathrm{i}&0\end{bmatrix}.$$

(ⅰ) 证明 $-I$ 是 $\mathbf{Q}$ 中唯一的阶为 2 的元素，而其他 $M\neq I$ 的元素满足 $M^2=-I$.

(ⅱ) 证明在矩阵乘法运算下，$\mathbf{Q}$ 是非阿贝尔群.

提示：注意 $A^2=-I=B^2$.

(ⅲ) 证明 $\mathbf{Q}$ 有唯一的阶为 2 的子群，它就是 $\mathbf{Q}$ 的中心.

2.60 设 G 的阶为 8，其元素

$$\pm 1,\pm \mathbf{i},\pm \mathbf{j},\pm \mathbf{k}$$

满足

$$\mathbf{i}^2=\mathbf{j}^2=\mathbf{k}^2=-1,\mathbf{ij}=\mathbf{k},\mathbf{jk}=\mathbf{i},\mathbf{ki}=\mathbf{j},$$
$$\mathbf{ij}=-\mathbf{ji},\mathbf{ik}=-\mathbf{ki},\mathbf{jk}=-\mathbf{kj}.$$

证明 $G\cong\mathbf{Q}$，反过来说，$\mathbf{Q}$ 就是这样的一个群.

2.61 证明四元数群 $\mathbf{Q}$ 和二面体群 D_8 的阶虽然都是 8，但不同构.

提示：用习题 2.42.

2.62 证明 A_4 是 S_4 的唯一的阶为 12 的子群.

提示：利用命题2.62(ⅱ).

2.63 证明对称群 $\Sigma(\pi_n)$ 与 S_n 的一个子群同构，其中 π_n 是有 n 个顶点的正多边形.

提示：运动 $\sigma\in\Sigma(\pi_n)$ 置换 π_n 的顶点 $X=\{v_1,\cdots,v_n\}$.

2.64 (ⅰ) 对每个群 G，证明由 $g\mapsto\gamma_g$ 给出的函数 $\Gamma:G\to\mathrm{Aut}(G)$ 是同态（其中 γ_g 是 g 形成的共轭.）

(ⅱ) 证明 $\ker\Gamma=Z(G)$，$\mathrm{im}\Gamma=\mathrm{Inn}(G)$. 由此推出 $\mathrm{Inn}(G)$是 $\mathrm{Aut}(G)$的子群.

(ⅲ) 证明 $\mathrm{Inn}(G)\lhd\mathrm{Aut}(G)$.

2.6 商群

整数模 m 的加法群的构造是从给定的群构造新群的一般方法的原型，这种新群叫做商群. 由 $\pi:a\mapsto[a]$ 定义的同态 $\pi:\mathbb{Z}\to\mathbb{I}_m$ 是满射，因此$\mathbb{I}_m$ 等于 $\mathrm{im}\pi$，从而$\mathbb{I}_m$ 的每个元素可表示为 $\pi(a)$的形式，其中 $a\in\mathbb{Z}$，且 $\pi(a)+\pi(b)=\pi(a+b)$. 这种用加法群$\mathbb{Z}$来描述加法群$\mathbb{I}_m$ 的方法可以推广到任意群上，且不必是阿贝尔群. 假设 $f:G\to H$ 是群 G 和 H 之间的满同态，因 f 是满射，所以 H 的每个元素可以表示为 $f(a)$，其中 $a\in G$，且 H 的运算由 $f(a)f(b)=f(ab)$ 给出，其中 $a,b\in G$. 现在 $K=\ker f$ 是 G 的正规子群，我们准备只用 G 和 K 来重新构成 $H=\mathrm{im}f$（以及满同态 $\pi:G\to H$）.

82

首先引入群 G 的一切非空子集的集合

$$\mathcal{S}(G)$$

上的一种运算. 设 X，$Y\in\mathcal{S}(G)$，定义

$$XY=\{xy:x\in X,y\in Y\}.$$

该运算是结合的：$X(YZ)$是一切 $x(yz)$的集合，其中 $x\in X,y\in Y,z\in Z$，$(XY)Z$ 是一切 $(xy)z$ 的集合，由 G 上的结合性可知，两者相同.

这种乘法的一个例子是单点子集$\{a\}$和子群$K \leqslant G$的积，这个积就是陪集aK.

作为第二个例子，我们证明如果H是G的任一子群，则

$$HH = H.$$

如果$h, h' \in H$，则因为子群在乘法下封闭，所以$hh' \in H$，由此$HH \subseteq H$. 关于反包含，如果$h \in H$，则$h = h1 \in HH$（因$1 \in H$），于是$H \subseteq HH$.

对于$\mathcal{S}(G)$中的两个子集X，Y，即使它们的构成元素不交换，它们自身仍可能交换. 例如，设$G = S_3, K = \langle(1\ 2\ 3)\rangle$. 现在$(1\ 2)$和$(1\ 2\ 3) \in K$不交换，但可断言$(1\ 2)K = K(1\ 2)$. 事实上，我们有习题2.50的逆命题.

引理 2.65 *群G的子群K是正规子群当且仅当对每个$g \in G$，*

$$gK = Kg.$$

由此，正规子群的右陪集也是左陪集.

证明 设$gk \in gK$. 因K是正规子群，所以$gkg^{-1} \in K$，比如$gkg^{-1} = k' \in K$，由此$gk = (gkg^{-1})g = k'g \in Kg$，从而$gK \subseteq Kg$. 关于反包含，设$kg \in Kg$. 因$K$是正规子群，$(g^{-1})k(g^{-1})^{-1} = g^{-1}kg \in K$，比如$g^{-1}kg = k'' \in K$，由此$kg = g(g^{-1}kg) = gk'' \in gK$，从而$Kg \subseteq gK$. 所以当$K \lhd G$时，$gK = Kg$.

反之，如果对每个$g \in G, gK = Kg$，则对每个$k \in K$，有$k' \in K$使得$gk = k'g$；即对一切$g \in G, gkg^{-1} \in K$，因此$K \lhd G$. ■

自然会问，当H和K两者都是子群时HK是否是子群. 一般来说，HK未必是子群. 例如，设$G = S_3, H = \langle(1\ 2)\rangle, K = \langle(1\ 3)\rangle$，则

$$HK = \{(1), (1\ 2), (1\ 3), (1\ 3\ 2)\}$$

不是子群，这只要注意到$4 \nmid 6$，如果HK是子群，则与拉格朗日定理矛盾.

[83]

定理 2.66 （i）*如果H和K都是群G的子群，且其中之一是正规子群，则HK是G的子群，且$HK = KH$.*

（ii）*如果H和K都是群G的正规子群，则HK也是正规子群.*

注 *习题2.72证明，如果H和K都是群G的子群，则HK是G的子群当且仅当$HK = KH$.*

证明 （i）首先假定$K \lhd G$，我们断言$HK = KH$. 如果$hk \in HK$，则因$K \lhd G, k' = hkh^{-1} \in K$，且

$$hk = hkh^{-1}h = k'h \in KH.$$

由此$HK \subseteq KH$. 关于反包含，有$kh = hh^{-1}kh = hk'' \in HK$.（如果$H \lhd G$，类似可证$HK = KH$.）

现在证明HK是子群. 因$1 \in H, 1 \in K$，所以有$1 = 1 \cdot 1 \in HK$；如果$hk \in HK$，则$(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$；如果$hk, h_1k_1 \in HK$，则$hkh_1k_1 \in HKHK = HHKK = HK$.

（ii）如果$g \in G$，则由引理2.65可得$gHK = HgK = HKg$，再由同一引理得$HK \lhd G$. ■

下面是由给定的群构造新群的基本方法.

定理 2.67 *设G/K表示G的子群K的一切左陪集的族. 如果K是正规子群，则对一切$a, b \in G$，*

$$aKbK = abK,$$

且G/K在此运算下是群.

注 *群G/K称为$G\bmod K$的**商群**，当G有限时，它的阶$|G/K|$就是指数$[G:K] = |G|/|K|$（可能这就是为什么叫它商群的理由）.*

证明 两个陪集$(aK)(bK)$的积也可看作$\mathcal{S}(G)$中4个元素的积，因此由$\mathcal{S}(G)$的结合性得

$$(aK)(bK) = a(Kb)K = a(bK)K = abKK = abK,$$

这是因为 K 是正规子群，根据引理2.65，对一切 $b \in K$ 有 $Kb = bK$，而 K 是子群，所以又有 $KK=K$. 由此 K 的两个陪集的积也是 K 的陪集，所以这就定义了 G/K 上的运算. 因为 $\mathcal{S}(G)$ 中的乘积是结合的，所以等式 $X(YZ) = (XY)Z$ 成立，特别地，X，Y，Z 是 K 的陪集时也成立，由此 G/K 上的运算是结合的. 幺元是陪集 $K=1K$，这是因为 $(1K)(bK) = 1bK = bK = b1K = (bK)(1K)$，而 aK 的逆是 $a^{-1}K$，这是因为 $(a^{-1}K)(aK) = a^{-1}aK = K = aa^{-1}K = (aK)(a^{-1}K)$. 所以 G/K 是群. ■

84

重要的是记住刚才证明了 G/K 中的积 $aKbK = abK$ 并不依赖于陪集的个别代表元，且代换定律成立：如果 $aK = a'K, bK = b'K$，则

$$aKbK = abK = a'b'K = a'Kb'K.$$

例 2.68 设 G 是加法群 $\mathbb{Z}$，$K = \langle m\rangle$ 是正整数 m 的一切倍数组成的(循环)子群，我们证明商群 G/K 正是 $\mathbb{I}_m$. 因 $\mathbb{Z}$ 是阿贝尔群，$\langle m\rangle$ 必是正规子群. 因为集合 $\mathbb{Z}/\langle m\rangle$ 和 $\mathbb{I}_m$ 由相同的元素构成，因此两集合相同：陪集 $a+\langle m\rangle$ 是同余类 $[a]$：

$$a+\langle m\rangle = \{a+km : k \in \mathbb{Z}\} = [a].$$

运算也相同：$\mathbb{Z}/\langle m\rangle$ 中的加法由

$$(a+\langle m\rangle)+(b+\langle m\rangle) = (a+b)+\langle m\rangle$$

给出，因 $a+\langle m\rangle = [a]$，上面的等式就是 $[a]+[b]=[a+b]$，而这正是 $\mathbb{I}_m$ 中的和. 所以 $\mathbb{I}_m$ 等于商群 $\mathbb{Z}/\langle m\rangle$. ■

还有一种方法来看待商群. 在引理2.40的证明中已经看到，定义 G 上的关系 $\equiv$ 为 $a \equiv b$，如果 $b^{-1}a \in K$，则关系 $\equiv$ 是 G 上的等价关系，它的等价类是 K 的陪集. 于是可把 G/K 的元素看作等价类，其乘法 $aKbK = abK$ 不依赖于代表元的选取.

提醒读者注意引理2.40(ⅰ)：如果 K 是 G 的子群，则两个陪集 aK 和 bK 相等当且仅当 $b^{-1}a \in K$. 特别地，如果 $b=1$，则 $aK=K$ 当且仅当 $a \in K$.

现在可以证明命题2.56(ⅱ)的逆命题.

系 2.69 每个正规子群 $K \lhd G$ 都是某个同态的核.

证明 定义自然映射 $\pi: G \to G/K$ 为 $\pi(a) = aK$. 用此记号可把公式 $aKbK = abK$ 重写为 $\pi(a)\pi(b) = \pi(ab)$，于是 π 是(满)同态. 因 K 是 G/K 中的幺元，由引理2.40(ⅰ)，

$$\ker\pi = \{a \in G : \pi(a) = K\} = \{a \in G : aK = K\} = K.$$ ■

下一定理证明每个同态导出一个同构，而商群仅仅是由同态象构成的. 诺特（E. Noether, 1882—1935）强调了这个事实的基本重要性.

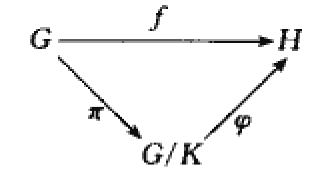
定理 2.70(第一同构定理) 如果 $f: G \to H$ 是同态，则

$$\ker f \lhd G \quad 且 \quad G/\ker f \cong \operatorname{im} f.$$

85

更详细地说，如果 $\ker f = K$ 且 $\varphi: G/K \to \operatorname{im} f \leqslant H$ 由 $\varphi: aK \mapsto f(a)$ 给出，则 φ 是同构.

注 下图描述了第一同构定理的证明，其中 $\pi: G \to G/K$ 是自然映射 $\pi: a \mapsto aK$.



证明 在命题2.56(ⅱ)中已经看到 $K=\ker f$ 是 G 的正规子群. 现在 φ 是合理定义的：如果 $aK = bK$，则有某个 $k \in K$ 使得 $a = bk$，又因 $f(k)=1$，由此 $f(a) = f(bk) = f(b)f(k) = f(b)$.

现在验证 φ 是同态. 因为 f 是同态且 $\varphi(aK) = f(a)$，所以

$$\varphi(aKbK) = \varphi(abK) = f(ab) = f(a)f(b) = \varphi(aK)\varphi(bK).$$

显然，$\mathrm{im}\varphi \leqslant \mathrm{im}f$. 关于反包含，如果 $y \in \mathrm{im}f$，则有某个 $a \in G$ 使得 $y = f(a)$，于是 $y = f(a) = \varphi(aK)$. 因此 φ 是满射.

最后证明 φ 是单射. 如果 $\varphi(aK) = \varphi(bK)$,则 $f(a) = f(b)$,因此 $1 = f(b)^{-1}f(a) = f(b^{-1}a)$,于是 $b^{-1}a \in \ker f = K$. 因此，根据引理2.40(ⅰ)，$aK=bK$，所以 φ 是单射. 以上就证明了 $\varphi: G/K \to \mathrm{im}f$ 是同构. ■

给定同态 $f: G \to H$，我们立即会问到它的核和象. 第一同构定理提供了同构 $G/\ker f \cong \mathrm{im}f$. 因为同构群之间没有显著的差别，所以由第一同构定理可知商群和同态象之间也没有显著的差别.

例 2.71 重新来看例 2.53，该例证明了任意两个阶为 m 的循环群同构. 设 $G=\langle a\rangle$是阶为 m 的循环群，定义函数 $f: \mathbb{Z} \to G$ 为对一切 $n\in\mathbb{Z}$，$f(n)=a^n$. 易知 f 是同态，f 还是满射(因为 a 是 G 的生成元)，而由定理 2.24，$\ker f = \{n \in \mathbb{Z}: a^n = 1\} = \langle m\rangle$. 第一同构定理给出同构 $\mathbb{Z}/\langle m\rangle \cong G$. 我们已经证明了每个阶为 m 的循环群同构于$\mathbb{Z}/\langle m\rangle$，因此任两个阶为 m 的循环群彼此同构. 例 2.68 又证明了$\mathbb{Z}/\langle m\rangle = \mathbb{I}_m$，从而每个 m 阶循环群同构于$\mathbb{I}_m$.

我们指出任意无限循环群同构于$\mathbb{Z}$，读者应不难证明这一点. ■

例 2.72 商群$\mathbb{R}/Z$是什么？由

$$f: x \mapsto e^{2\pi i x}$$

定义 $f: \mathbb{R} \to S^1$，其中 S^1 是圆群. 根据正弦和余弦的加法公式得 $f(x+y) = f(x)f(y)$，即 f 是同态. 映射 f 是满射，$\ker f$ 由所有满足 $e^{2\pi i x} = \cos 2\pi x + i\sin 2\pi x = 1$ 的 $x \in \mathbb{R}$ 组成，即 $\cos 2\pi x = 1$，$\sin 2\pi x = 0$，而 $\cos 2\pi x = 1$ 迫使 x 必须是整数，因为 $1 \in \ker f$，所以 $\ker f = \mathbb{Z}$. 第一同构定理给出 [86]

$$\mathbb{R}/\mathbb{Z} \cong S^1.$$

这是例1.55(ⅰ)的群论版本. ■

这里有一个有用的计数结果.

命题 2.73(乘积公式) *如果 H 和 K 是有限群 G 的子群，则*

$$|HK||H \cap K| = |H||K|,$$

其中 $HK = \{hk : h \in H, k \in K\}$.

注 *子集 HK 未必是 G 的子群，然而命题 2.66 证明，如果 $H \lhd G$ 或 $K \lhd G$，则 HK 是子群(也可参见习题 2.72).*

证明 定义函数 $f: H \times K \to HK$ 为 $f: (h,k) \mapsto hk$. 显然，f 是满射. 只需证明对每个 $x \in HK$，$|f^{-1}(x)| = |H \cap K|$，其中 $f^{-1}(x) = \{(h,k) \in H \times K : hk = x\}$. [因为 $H \times K$ 是不相交并 $\bigcup_{x \in HK} f^{-1}(x)$.]

我们断言，如果 $x=hk$，则

$$f^{-1}(x) = \{(hd, d^{-1}k) : d \in H \cap K\}.$$

因为 $f(hd, d^{-1}k) = hdd^{-1}k = hk = x$，所以每个 $(hd, d^{-1}k) \in f^{-1}(x)$. 关于反包含，设 $(h',k') \in f^{-1}(x)$，于是 $h'k' = hk$，从而 $h^{-1}h' = kk'^{-1} \in H \cap K$，把这个元素叫做 d，则 $h' = hd, k' = d^{-1}k$，因此 (h',k') 位于右端的集合中. 因 $d \mapsto (hd, d^{-1}k)$，是双射，所以

$$|f^{-1}(x)| = |\{(hd, d^{-1}k) : d \in H \cap K\}| = |H \cap K|.$$ ■

下面两个结果是第一同构定理的推论.

定理 2.74(第二同构定理) 如果 H，K 是群 G 的子群满足 $H \lhd G$，则 HK 是子群，$H \cap K \lhd K$，并且

$$K/(H \cap K) \cong HK/H.$$

证明 因 $H \lhd G$，命题 2.66 证明 HK 是子群. H 在 HK 中的正规性来自下述更一般的事实：如果 $H \leqslant S \leqslant G$，$H$ 是 G 的正规子群，则 H 也是 S 的正规子群（如果对每个 $g \in G, ghg^{-1} \in H$，则特别地，对每个 $g \in S, ghg^{-1} \in H$）.

87

现在证明每个陪集 $xH \in HK/H$ 都有某个 $k \in K$ 使它具有 kH 的形式. 当然，$xH = hkH$，其中 $h \in H$，$k \in K$. 但有某个 $h' \in H$ 使得 $hk = kk^{-1}hk = kh'$，于是 $hkH = kh'H = kH$. 由此，由 $f: k \mapsto kH$ 给出的函数 $f: K \to HK/H$ 是满射. 而且，因为它是自然映射 $\pi: G \to G/H$ 的限制，所以 f 是同态. 因 $\ker\pi = H$，从而 $\ker f = H \cap K$ 且 $H \cap K$ 是 K 的正规子群. 由第一同构定理得 $K/(H \cap K) \cong HK/H$. ■

第二同构定理可推出乘积公式的一个特殊情形，即两个子群之一是正规子群时的情形：如果 $K/(H \cap K) \cong HK/H$，则 $|K/(H \cap K)| = |HK/H|$，因此 $|HK||H \cap K| = |H||K|$.

定理 2.75(第三同构定理) 如果 H，K 是群 G 的正规子群且 $K \leqslant H$，则 $H/K \lhd G/K$，且

$$(G/K)/(H/K) \cong G/H.$$

证明 定义 $f: G/K \to G/H$ 为 $f: aK \mapsto aH$. 注意 f 是(合理定义的)函数，这是因为如果 $a' \in G$ 且 $a'K = aK$，则 $a^{-1}a' \in K \leqslant H$，因此 $aH = a'H$. 易知 f 是满同态.

因 $aH = H$ 当且仅当 $a \in H$，所以 $\ker f = H/K$，由此 H/K 是 G/K 的正规子群. 因 f 是满射，由第一同构定理得

$$(G/K)/(H/K) \cong G/H.$$ ■

容易记住第三同构定理：在分式 $(G/K)/(H/K)$ 中可消去 K. 证明了第三同构定理之后，我们可以更好地欣赏第一同构定理. 商群 $(G/K)/(H/K)$ 由代表元本身为 (G/K 的)陪集的(H/K 的) 陪集所构成. 第三同构定理的直接证明是非常麻烦的.

命题 2.76(对应定理) 设 G 是群，$K \lhd G$，并设 $\pi: G \to G/K$ 是自然映射，则

$$S \mapsto \pi(S) = S/K$$

是 $\mathrm{Sub}(G;K)$ 和 $\mathrm{Sub}(G/K)$ 之间的双射，其中 $\mathrm{Sub}(G;K)$ 是 G 的包含 K 的一切子群 S 的族，$\mathrm{Sub}(G/K)$ 是 G/K 的一切子群的族. 如果用 S^* 记 S/K，则

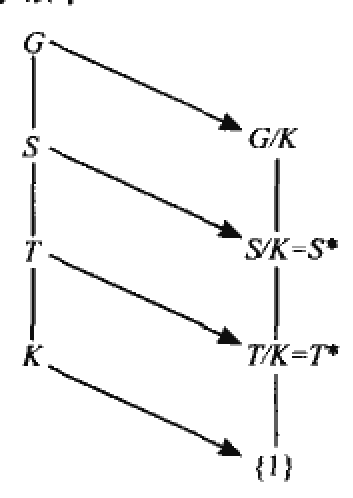
$$T \leqslant S \leqslant G \quad \text{当且仅当 } T^* \leqslant S^*, \text{此时} [S:T] = [S^*:T^*],$$

且

88

$$T \lhd S \quad \text{当且仅当 } T^* \lhd S^*, \text{此时 } S/T \cong S^*/T^*.$$

注 下图是记住这个定理的一种方法：



证明 定义 Φ: $\mathrm{Sub}(G;K)\to\mathrm{Sub}(G/K)$ 为 $S\mapsto S/K$（容易验证：如果 S 是 G 的包含 K 的子群，则 S/K 是 G/K 的子群）.

为证明 Φ 是单射，先证明如果 $K\leqslant S\leqslant G$，则 $\pi^{-1}\pi(S)=S$. 由命题1.50（ⅳ），恒有 $S\subseteq\pi^{-1}\pi(S)$. 关于反包含，设 $a\in\pi^{-1}\pi(S)$，于是对某个 $s\in S$ 有 $\pi(a)=\pi(s)$. 由此 $as^{-1}\in\ker\pi=K$，因此有某个 $k\in K$ 使得 $a=sk$. 但 $K\leqslant S$，所以 $a=sk\in S$.

现在假定 $\pi(S)=\pi(S')$，其中 S 和 S' 都是 G 的包含 K 的子群，则 $\pi^{-1}\pi(S)=\pi^{-1}\pi(S')$，根据上一段刚刚证明的结果得 $S=S'$，因此 Φ 是单射.

为证明 Φ 是满射，设 U 是 G/K 的子群，则 $\pi^{-1}(U)$ 是 G 的包含 $K=\pi^{-1}(\{1\})$ 的子群，并由命题1.50（ⅱ）得 $\pi(\pi^{-1}(U))=U$.

命题1.50（ⅰ）表明 $T\leqslant S\leqslant G$ 蕴涵 $T/K=\pi(T)\leqslant\pi(S)=S/K$. 反之，假定 $T/K\leqslant S/K$. 如果 $t\in T$，则 $tK\in T/K\leqslant S/K$，从而有某个 $s\in S$ 使得 $tK=sK$. 因此有某个 $k\in K\leqslant S$ 使得 $t=sk$，于是 $t\in S$.

为证明 $[S:T]=[S^*:T^*]$，只需证明在一切形如 sT 的陪集族和一切形如 s^*T^* 的陪集族之间存在双射，其中 $s\in S, s^*\in S^*$. 读者可以验证 $sT\mapsto\pi(s)T^*$ 就是这样的一个双射. 当 G 有限时，可证明 $[S:T]=[S^*:T^*]$ 如下：

$$\begin{aligned}[S^*:T^*]&=|S^*|/|T^*|\\&=|S/K|/|T/K|\\&=(|S|/|K|)/(|T|/|K|)\\&=|S|/|T|\\&=[S:T].\end{aligned}$$

89

如果 $T\lhd S$，则由第三同构定理知，$T/K\lhd S/K$ 且 $(S/K)/(T/K)\cong S/T$，即 $S^*/T^*\cong S/T$. 剩下的是证明：如果 $T^*\lhd S^*$，则 $T\lhd S$，也就是要证明如果 $t\in T$，$s\in S$，则 $sts^{-1}\in T$. 现在

$$\pi(sts^{-1})=\pi(s)\pi(t)\pi(s)^{-1}\in\pi(s)T^*\pi(s)^{-1}=T^*,$$

因此，$sts^{-1}\in\pi^{-1}(T^*)=T$. ■

在处理商群的时候，通常不明确地提及对应定理而说 G/K 的每个子群形如 S/K，其中 $S\leqslant G$ 是包含 K 的唯一子群.

例 2.77 设 $G=\langle a\rangle$ 是 30 阶的循环群. 如果定义 $\pi:\mathbb{Z}\to G$ 为 $\pi(n)=a^n$，则 $\ker\pi=\langle 30\rangle$. 子群 $\langle 30\rangle\leqslant\langle 15\rangle\leqslant\langle 5\rangle\leqslant\mathbb{Z}$ 对应子群

$$\{1\}=\langle a^{30}\rangle\leqslant\langle a^{15}\rangle\leqslant\langle a^5\rangle\leqslant\langle a\rangle.$$

此外，商群是

$$\frac{\langle a^{15}\rangle}{\langle a^{30}\rangle}\cong\frac{\langle 15\rangle}{\langle 30\rangle}\cong\mathbb{I}_2,\frac{\langle a^5\rangle}{\langle a^{15}\rangle}\cong\frac{\langle 5\rangle}{\langle 15\rangle}\cong\mathbb{I}_3,\frac{\langle a\rangle}{\langle a^5\rangle}\cong\frac{\mathbb{Z}}{\langle 5\rangle}\cong\mathbb{I}_5$$ ■

命题 2.78 如果 G 是有限阿贝尔群，d 是 $|G|$ 的因数，则 G 含有 d 阶子群.

证明 对 $n=|G|$ 用归纳法证明关于 $|G|$ 的素因数 p 结论成立. 基础步 $n=1$ 为真，因为 1 没有素因数. 关于归纳步，选取阶为 $k>1$ 的元素 $a\in G$. 如果 $p\mid k$，比如 $k=p\ell$，则习题 2.23 说 a^ℓ 的阶为 p. 如果 $p\nmid k$，考虑循环子群 $H=\langle a\rangle$. 因 G 是阿贝尔群，所以 $H\lhd G$，因此存在商群 G/H. 注意到 $|G/H|=n/k$ 被 p 整除，归纳假设给出 p 阶元素 $bH\in G/K$. 如果 b 的阶为 m，则习题 2.47（ⅰ）给出 $p\mid m$. 回到第一种情形.

设 d 是 $|G|$ 的任一因数，且 p 是 d 的素因数. 刚才已知有阶为 p 的子群 $S\leqslant G$，因 G 是阿贝

尔群，所以 $S\lhd G$ 且 G/S 是 n/p 阶群. 对 $|G|$ 用归纳法可知 G/S 有 d/p 阶子群 H^*，对应定理给出某个包含 S 的子群 H 使得 $H^*=H/S$，且 $|H|=|H^*||S|=d$. ■

下面是以两个给定的群构造新群的一种方法.

定义 如果 H 和 K 是群，则全体有序对 (h,k) 的集合（其中 $h\in H,k\in K$）配置运算

$$(h,k)(h',k')=(hh',kk')$$

称为 H 和 K 的**直积**，记为 $H\times K$.

容易验证直积 $H\times K$ 是群 [幺元是 $(1,1)$, $(h,k)^{-1}=(h^{-1},k^{-1})$].

90

现在把第一同构定理运用到直积上.

命题 2.79 设 G 和 G' 是群，并设 $K\lhd G,K'\lhd G'$ 是正规子群，则 $K\times K'\lhd G\times G'$，且有同构

$$(G\times G')/(K\times K')\cong(G/K)\times(G'/K').$$

证明 设 $\pi:G\to G/K,\pi':G'\to G'/K'$ 是自然映射，容易验证由

$$f:(g,g')\mapsto(\pi(g),\pi'(g'))=(gK,g'K')$$

给出的 $f:G\times G'\to(G/K)\times(G'/K')$ 是满同态，其中 $\ker f=K\times K'$. 现在第一同构定理给出命题要求的同构. ■

命题 2.80 如果群 G 包含正规子群 H 和 K 满足 $H\cap K=\{1\},HK=G$，则 $G\cong H\times K$.

证明 首先证明 $g\in G$ 有唯一的因子分解 $g=hk$，其中 $h\in H$，$k\in K$. 如果 $hk=h'k'$，则 $h'^{-1}h=k'k^{-1}\in H\cap K=\{1\}$，所以 $h'=h,k'=k$. 现在可定义函数 $\varphi:G\to H\times K$ 为 $\varphi(g)=(h,k)$，其中 $g=hk,h\in H,k\in K$. 为了确定 φ 是否为同态，设 $g'=h'k'$，从而 $gg'=hkh'k'$，因此 $\varphi(gg')=\varphi(hkh'k')$，但这个形式并不适合计算. 如果已知对 $h\in H$ 和 $k\in K$ 有 $hk=kh$，则可继续推导如下：

$$\begin{aligned}\varphi(hkh'k')&=\varphi(hh'kk')\\&=(hh',kk')\\&=(h,k)(h',k')\\&=\varphi(g)\varphi(g)'.\end{aligned}$$

设 $h\in H$，$k\in K$. 因 K 是正规子群，所以 $(hkh^{-1})k^{-1}\in K$；因 H 是正规子群，所以 $h(kh^{-1}k^{-1})\in H$. 但 $H\cap K=\{1\}$，因此 $hkh^{-1}k^{-1}=1$，从而 $hk=kh$. 最后证明同态 φ 是同构. 如果 $(h,k)\in H\times K$，则由 $g=hk$ 定义的元素 $g\in G$ 满足 $\varphi(g)=(h,k)$，因此 φ 是满射. 如果 $\varphi(g)=(1,1)$，则 $g=1$，从而 $\ker\varphi=1$ 且 φ 是单射. 所以 φ 是同构. ■

注 必须假定子群 H 和 K 两者都是正规子群. 例如，S_3 有子群 $H=\langle(1\ 2\ 3)\rangle$ 和 $K=\langle(1\ 2)\rangle$. 现在 $H\lhd S_3,H\cap K=\{1\}$ 且 $HK=S_3$，但 $S_3\ncong H\times K$（因为直积是阿贝尔群），当然 K 不是 S_3 的正规子群.

定理 2.81 如果 m 和 n 互素，则

91

$$\mathbb{I}_{mn}\cong\mathbb{I}_m\times\mathbb{I}_n.$$

证明 设 $a\in\mathbb{Z}$，记它在 $\mathbb{I}_m$ 中的同余类为 $[a]_m$. 读者可验证由 $a\mapsto([a]_m,[a]_n)$ 给出的函数 $f:\mathbb{Z}\to\mathbb{I}_m\times\mathbb{I}_n$ 是同态. 我们断言 $\ker f=\langle mn\rangle$. 显然 $\langle mn\rangle\leqslant\ker f$. 关于反包含，设 $a\in\ker f$，则 $[a]_m=[0]_m,[a]_n=[0]_n$，即 $a\equiv 0\bmod m,a\equiv 0\bmod n$，也就是 $m\mid a,n\mid a$. 因 m 和 n 互素，所以 $mn\mid a$，从而 $a\in\langle mn\rangle$，即 $\ker f\leqslant\langle mn\rangle$，从而 $\ker f=\langle mn\rangle$. 第一同构定理给出 $\mathbb{Z}/\langle mn\rangle\cong\operatorname{im}f$

$\leqslant \mathbb{I}_m \times \mathbb{I}_n$，但 $\mathbb{Z}/\langle mn\rangle \cong \mathbb{I}_{mn}$ 有 mn 个元素，它和 $\mathbb{I}_m \times \mathbb{I}_n$ 的元素个数相等，因此断定 f 是满射. ■

例如，由命题 2.81 可得 $\mathbb{I}_6 \cong \mathbb{I}_2 \times \mathbb{I}_3$．注意，如果 m 和 n 不互素，就不存在同构. 例如 $\mathbb{I}_4 \not\cong \mathbb{I}_2 \times \mathbb{I}_2$，因为$\mathbb{I}_4$ 有 4 阶元素，而直积(它同构于四群 **V**) 没有这样的元素.

依据命题 2.34，如果 $\langle a\rangle \cong \mathbb{I}_n$，就可以说元素 $a\in G$ 的阶为 n. 现在定理 2.81 可解释为：如果 a 和 b 可交换，而且它们的阶 m 和 n 互素，则 ab 的阶为 mn. 下面给出这个结果的直接证明.

命题 2.82 *设 G 是群，元素 a，$b\in G$ 可交换，它们分别有阶 m 和 n. 如果 $(m,n)=1$，则 ab 的阶为 mn.*

证明 因 a 和 b 可交换，对一切 r 有 $(ab)^r = a^r b^r$，因此 $(ab)^{mn} = a^{mn}b^{mn} = 1$. 于是只需证明：如果 $(ab)^k = 1$，则 $mn \mid k$. 如果 $1 = (ab)^k = a^k b^k$，则 $a^k = b^{-k}$. 因 a 的阶为 m，所以有 $1 = a^{mk} = b^{-mk}$. 因 b 的阶为 n，根据定理 2.24 有 $n \mid mk$. 然而由于 $(m,n)=1$，因此系 1.11 给出 $n \mid k$. 同样可推出 $m \mid k$. 最后，习题 1.19 证明 $mn \mid k$. 所以 $mn \leqslant k$，且 mn 是 ab 的阶. ■

系 2.83 *如果 $(m, n) = 1$，则 $\phi(mn) = \phi(m)\phi(n)$，其中 ϕ 是欧拉 ϕ-函数.*

证明[⊖] 定理 2.81 证明由 $[a]\mapsto([a]_m,[a]_n)$ 给出的函数 $f: \mathbb{I}_{mn}\to\mathbb{I}_m\times\mathbb{I}_n$ 是同构. 如果能够证明 $f(U(\mathbb{I}_{mn})) = U(\mathbb{I}_m)\times U(\mathbb{I}_n)$，便可导出结果如下：

$$\phi(mn) = |U(\mathbb{I}_{mn})| = |f(U(\mathbb{I}_{mn}))|$$
$$= |U(\mathbb{I}_m)\times U(\mathbb{I}_n)| = |U(\mathbb{I}_m)|\cdot|U(\mathbb{I}_n)| = \phi(m)\phi(n).$$

如果 $[a]\in U(\mathbb{I}_{mn})$，则有某个 $b\in\mathbb{I}_{mn}$ 使得 $[a][b]=[1]$，且

$$f([ab]) = ([ab]_m,[ab]_n) = ([a]_m[b]_m,[a]_n[b]_n)$$
$$= ([a]_m,[a]_n)([b]_m,[b]_n) = ([1]_m,[1]_n).$$

因此，$[1]_m = [a]_m[b]_m, [1]_n = [a]_n[b]_n$，于是 $f([a]) = ([a]_m,[a]_n) \in U(\mathbb{I}_m)\times U(\mathbb{I}_n)$，从而 $f(U(\mathbb{I}_{mn}))\subseteq U(\mathbb{I}_m)\times U(\mathbb{I}_n)$.

关于反包含，设 $f([c]) = ([c]_m,[c]_n)\in U(\mathbb{I}_m)\times U(\mathbb{I}_n)$，我们必须证明 $[c]\in U(\mathbb{I}_{mn})$. 存在 $[d]_m\in\mathbb{I}_m$ 使得 $[c]_m[d]_m = [1]_m$，又存在 $[e]_n\in\mathbb{I}_n$ 使得 $[c]_n[e]_n = [1]_n$. 因 f 是满射，所以存在 $b\in\mathbb{Z}$ 使得 $([b]_m,[b]_n) = ([d]_m,[e]_n)$，于是 [92]

$$f([1]) = ([1]_m,[1]_n) = ([c]_m[b]_m,[c]_n[b]_n) = f([c][b]).$$

因 f 是单射，所以 $[1] = [c][b]$，从而 $[c]\in U(\mathbb{I}_{mn})$. ■

系 2.84 (i) *如果 p 是素数，则 $\phi(p^e) = p^e - p^{e-1} = p^e\left(1-\frac{1}{p}\right)$.*

(ii) *如果 $n = p_1^{e_1}\cdots p_t^{e_t}$ 是 n 的素因数分解，其中 p_1，…，p_t 是不同的素数，则*

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_t}\right).$$

证明概要 (i) 成立是因为 $(k,p^e)=1$ 当且仅当 $p\nmid k$. (ii) 由系 2.83 导出. ■

引理 2.85 *在 n 阶循环群中，对于 n 的每个因数 d，有唯一的 d 阶子群，且该子群是循环群.*

证明 设 $G=\langle a\rangle$. 如果 $n=cd$，我们证明 a^c 的阶为 d (从而 $\langle a^c\rangle$ 是 d 阶子群). 显然，$(a^c)^d = a^{cd} = a^n = 1$，我们断言 d 是最小的这种幂. 如果 $(a^c)^r = 1$，则 $n \mid cr$ [定理 2.24]，因此有某个整数 s 使得 $cr = ns = dcs$，从而 $r = ds \geqslant d$.

为了证明唯一性，假定 $\langle x\rangle$ 是 d 阶子群(回忆习题 2.34，循环群的每个子群都是循环群). 现在

⊖ 习题 3.50 有较简洁的证明.

$x=a^m, 1=x^d=a^{md}$，因此有某个整数 k 使得 $md=nk$，于是 $x=a^m=(a^{n/d})^k=(a^c)^k$，从而 $\langle x\rangle\leqslant\langle a^c\rangle$. 因为两个子群有相同的阶 d，所以 $\langle x\rangle=\langle a^c\rangle$. ■

定义群 G 上的等价关系为 $x\equiv y$ 如果 $\langle x\rangle=\langle y\rangle$；即如果 x 和 y 为同一循环子群的生成元，则 x 和 y 等价. 记包含元素 x 的等价类为 gen(C)，其中 $C=\langle x\rangle$，于是 gen(C) 由 C 的一切生成元组成. 照常，等价类形成划分，因此 G 是不相交并：

$$G=\bigcup_C \operatorname{gen}(C),$$

其中 C 遍历 G 的一切循环子群. 在定理2.33(ⅱ)中证明了

$$|\operatorname{gen}(C)|=\phi(|C|),$$

其中 ϕ 是欧拉 ϕ-函数.

下一定理稍后将用来证明乘法群 $\mathbb{I}_p^\times$ 是循环群.

[93]

定理 2.86 *n 阶群 G 是循环群当且仅当对 n 的每个因数 d，最多有一个 d 阶循环子群.*

证明 如果 G 是循环群，则由引理 2.85 可得结果. 反之，把 G 写作不相交并：

$$G=\bigcup_C \operatorname{gen}(C).$$

由此，$n=|G|=\sum|\operatorname{gen}(C)|$，其中和式是对 G 的一切循环子群 C 取和：

$$n=\sum_C|\operatorname{gen}(C)|=\sum_C\phi(|C|).$$

根据假设，对 n 的任一因数 d，群 G 最多有一个 d 阶循环子群，所以

$$n=\sum_C|\operatorname{gen}(C)|=\sum_C\phi(|C|)\leqslant\sum_{d\mid n}\phi(d)=n,$$

上面最后一个等式是系 1.39. 因此对 n 的每个因数 d，上式中的 $\phi(d)$ 必由 $|\operatorname{gen}(C)|$ 产生，其中 C 是 G 的某个 d 阶循环子群. 特别地，$\phi(n)$ 出现在上式中，因此有 n 阶循环子群，从而 G 是循环群. ■

下面是上一定理在阿贝尔群情形下的证明(由 D. Leep 提供).

定理 *如果 G 是 n 阶阿贝尔群，且对 n 的每个素因数 p 最多有一个阶为 p 的循环子群，则 G 是循环群.*

证明 对 $n=|G|$ 用归纳法证明. 基础步 $n=1$ 显然成立. 关于归纳步，首先注意到 G 的子群继承了假设. 我们断言在 G 中有某个元素 x，它的阶是 $|G|$ 的素因数 p. 选取 $y\in G$ 且 $y\neq 1$，由拉格朗日定理知，它的阶 k 是 $|G|$ 的因数，于是有某个素数 p 使得 $k=pm$. 由习题 2.23，元素 $x=y^m$ 的阶为 p. 定义 $\theta: G\to G$ 为 $\theta: g\mapsto g^p$ (因 G 是阿贝尔群，所以 θ 是同态). 现在 $x\in\ker\theta$，因此 $|\ker\theta|\geqslant p$. 如果 $|\ker\theta|>p$，则有多于 p 个元素 $g\in G$ 满足 $g^p=1$，这迫使 G 中 p 阶子群不止一个，所以 $|\ker\theta|=p$. 由第一同构定理，$G/\ker\theta\cong\operatorname{im}\theta\leqslant G$. 因此，$\operatorname{im}\theta$ 是 G 的满足归纳假设的 n/p 阶子群，所以有一个元素 $z\in\operatorname{im}\theta$ 使得 $\operatorname{im}\theta=\langle z\rangle$. 此外，因 $z\in\operatorname{im}\theta$，所以有 $b\in G$ 使得 $z=b^p$. 现在有两种情形. 如果 $p\nmid n/p$，则由命题 2.82，xz 的阶为 $p\cdot n/p=n$，从而 $G=\langle xz\rangle$. 如果 $p\mid n/p$，则习题 2.24 证明 b 的阶为 n，从而 $G=\langle b\rangle$. ■

如果 G 不是阿贝尔群，则这个定理可能不成立. 四元数群 $\mathbf{Q}$ 是 8 阶非阿贝尔群，它恰好有一个 2 阶（循环）子群.

习题

2.65 证明 $U(\mathbb{I}_9)\cong\mathbb{I}_6, U(\mathbb{I}_{15})\cong\mathbb{I}_4\times\mathbb{I}_2$.

2.66 (ⅰ) 设 H 和 K 是群，不用第一同构定理证明：$H^* = \{(h,1): h \in H\}$ 和 $K^* = \{(1,k): k \in K\}$ 是 $H\times G$的正规子群，其中 $H \cong H^*, K \cong K^*$，并且由 $f(h) = (h,1)K^*$ 定义的 $f: H \to (H\times K)/K^*$ 是同构.

94

(ⅱ) 用第一同构定理证明 $K^* \lhd H \times K$，且

$$(H \times K)/K^* \cong H.$$

提示：考虑由 $f:(h,k) \mapsto h$ 定义的函数 $f: H\times K \to H$.

2.67 (ⅰ) 证明 $\mathrm{Aut}(\mathbf{V}) \cong S_3$，$\mathrm{Aut}(S_3) \cong S_3$. 由此可知不同构的群可以有同构的自同构群.

(ⅱ) 证明 $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{I}_2$. 由此可知无限群可能有有限的自同构群.

2.68 如果 G 是群，且 $\mathrm{Aut}(G) = \{1\}$，证明 $|G| \leqslant 2$.

2.69 证明：如果 G 是群且 $G/Z(G)$是循环群，其中 $Z(G)$表示 G 的中心，则 G 是阿贝尔群.

提示：如果 $G/Z(G)$是循环群，证明其生成元给出 $Z(G)$之外的一个元素，它和 G 中的每个元素都可交换.

2.70 (ⅰ) 证明 $\mathbf{Q}/Z(\mathbf{Q}) \cong \mathbf{V}$，其中 $\mathbf{Q}$ 是四元数群，$\mathbf{V}$ 是四群. 由此可知，一个群关于其中心的商群可以是阿贝尔群.

(ⅱ) 证明 $\mathbf{Q}$ 没有与 $\mathbf{V}$ 同构的子群. 由此可知，商群 $\mathbf{Q}/Z(\mathbf{Q})$与 $\mathbf{Q}$ 的子群不同构.

2.71 设 G 是有限群且 $K \lhd G$，如果 $(|K|, [G:K]) = 1$，证明 K 是 G 的唯一 $|K|$ 阶子群.

提示：如果 $H \leqslant G$ 且 $|H| = |K|$，在 G/K 中 H 的元素会发生什么情况？

2.72 如果 H 和 K 都是群 G 的子群，证明 HK 是 G 的子群当且仅当 $HK = KH$.

提示：用 $H \subseteq HK$ 和 $K \subseteq HK$ 的事实.

2.73 设 G 是群并把 $G\times G$ 看作 G 和其自身的直积. 如果乘法 $\mu: G\times G \to G$ 是群同态，证明 G 必是阿贝尔群.

2.74 把定理 2.81 推广如下：设 G 是 mn 阶有限(加法) 阿贝尔群，其中$(m,n)=1$，定义

$$G_m = \{g \in G: 阶(g) \mid m\}, \quad G_n = \{h \in G: 阶(h) \mid n\}.$$

(ⅰ) 证明 G_m 和 G_n 是子群，且 $G_m \cap G_n = \{0\}$.

(ⅱ) 证明 $G = G_m + G_n = \{g + h: g \in G_m, h \in G_n\}$.

(ⅲ) 证明 $G \cong G_m \times G_n$.

2.75 设 G 是有限群，p 是素数，H 是 G 的正规子群. 证明：如果 $|H|$ 和 $|G/H|$ 两者都是 p 的幂，则 $|G|$ 也是 p 的幂.

2.76 如果 H 和 K 都是群 G 的正规子群，且 $HK=G$. 证明

$$G/(H \cap K) \cong (G/H) \times (G/K).$$

提示：定义 $\varphi: G \to (G/H)\times(G/K)$ 为 $x \mapsto (xH, xK)$，则 $\ker\varphi = H \cap K$. 又因 $G=HK$，所以

$$\bigcup_a aH = HK = \bigcup_b bK.$$

95

定义：如果 $H_1, \cdots, H_n$ 是群，则它们的**直积**

$$H_1 \times \cdots \times H_n$$

是指全体 n 元组 $(h_1, \cdots, h_n)$ 的集合，(其中对所有 i，$h_i \in H_i$) 并配置坐标状态的乘法：

$$(h_1, \cdots, h_n)(h_1', \cdots, h_n') = (h_1 h_1', \cdots, h_n h_n').$$

2.77 (ⅰ) 推广定理 2.81：证明如果整数 m 的素因数分解是 $m = p_1^{e_1} \cdots p_n^{e_n}$，则

$$\mathbb{I}_m \cong \mathbb{I}_{p_1^{e_1}} \times \cdots \times \mathbb{I}_{p_n^{e_n}}$$

(ⅱ) 推广系 2.83：证明如果整数 m 的素因数分解是 $m = p_1^{e_1} \cdots p_n^{e_n}$，则

$$U(\mathbb{I}_m) \cong U(\mathbb{I}_{p_1^{e_1}}) \times \cdots \times U(\mathbb{I}_{p_n^{e_n}}).$$

2.7 群的作用

置换组成的群把我们带到抽象群，下面的结果属于凯莱，说明抽象群并没有离开置换很远.

定理 2.87(凯莱) 每个群 G 同构于对称群 S_G 的一个子群. 特别地，如果 $|G|=n$，则 G 同构于 S_n 的一个子群.

证明 对每个 $a\in G$，定义"平移" $\tau_a: G\to G$ 为对每个 $x\in G, \tau_a(x)=ax$ (如果 $a\neq 1$，则 τ_a 不是同态). 对 $a, b\in G$，由结合性，$(\tau_a\circ\tau_b)(x)=\tau_a(\tau_b(x))=\tau_a(bx)=a(bx)=(ab)x$. 于是

$$\tau_a\tau_b=\tau_{ab}.$$

由此因为 τ_a 的逆是 $\tau_{a^{-1}}$：

$$\tau_a\tau_{a^{-1}}=\tau_{aa^{-1}}=\tau_1=1_G=\tau_{a^{-1}a},$$

所以每个 τ_a 都是双射，从而 $\tau_a\in S_G$.

定义 $\varphi: G\to S_G$ 为 $\varphi(a)=\tau_a$，重写得

$$\varphi(a)\varphi(b)=\tau_a\tau_b=\tau_{ab}=\varphi(ab),$$

由此 φ 是同态. 最后，φ 是单射. 如果 $\varphi(a)=\varphi(b)$，则 $\tau_a=\tau_b$，因此对一切 $x\in G$，$\tau_a(x)=\tau_b(x)$，特别是当 $x=1$ 时可得所要的 $a=b$.

最后的陈述由习题 2.39 得到，该题说如果 X 是满足 $|X|=n$ 的集合，则 $S_X\cong S_n$. ■

读者可能注意到在凯莱定理的证明中，置换 τ_a 就是 G 的乘法表中的第 a 行.

坦白地说，对凯莱定理本身的兴趣是一般的. 然而，在更大的框架中进行的同样的证明却是更重要的.

96

定理 2.88(陪集上的表示) 设 G 是群，H 是 G 的有有限指数 n 的子群，则存在同态 $\varphi: G\to S_n$ 使得 $\ker\varphi\leqslant H$.

证明 即使 H 可能不是正规子群，仍然记 H 在 G 中的一切陪集的族为 G/H.

对每个 $a\in G$，定义"平移" $\tau_a: G/H\to G/H$ 为对每个 $x\in G, \tau_a(xH)=axH$. 对 $a,b\in G$，由结合性，

$$(\tau_a\circ\tau_b)(xH)=\tau_a(\tau_b(xH))=\tau_a(bxH)=a(bxH)=(ab)xH,$$

于是

$$\tau_a\tau_b=\tau_{ab}.$$

由此因为 τ_a 的逆是 $\tau_{a^{-1}}$：

$$\tau_a\tau_{a^{-1}}=\tau_{aa^{-1}}=\tau_1=1_{G/H}=\tau_{a^{-1}}\tau_a,$$

所以每个 τ_a 都是双射，从而 $\tau_a\in S_{G/H}$. 定义 $\varphi: G\to S_{G/H}$ 为 $\varphi(a)=\tau_a$，重写得

$$\varphi(a)\varphi(b)=\tau_a\tau_b=\tau_{ab}=\varphi(ab),$$

由此 φ 是同态. 最后，如果 $a\in\ker\varphi$，则 $\varphi(a)=1_{G/H}$，因此对一切 $x\in G, \tau_a(xH)=xH$，特别当 $x=1$ 时，$aH=H$，由引理2.40(i)，$a\in H$. 因 $|G/H|=n$，习题 2.39 给出这一结果，从而 $S_{G/H}\cong S_n$. ■

当 $H=\{1\}$ 时，就是凯莱定理.

现在将对阶最多为 7 的群进行分类. 由例 2.53，每个阶为素数 p 的群同构于$\mathbb{I}_p$，因此，不计同构，p 阶群只有一个. 最多为 7 的阶中，2，3，5，7 四个是素数，所以只需看 4 阶和 6 阶.

命题 2.89 *每个 4 阶群 G 或者同构于$\mathbb{I}_4$，或者同构于四群 $\mathbf{V}$. 此外，$\mathbb{I}_4$ 和 $\mathbf{V}$ 不同构.*

证明 由拉格朗日定理，G 的每个不等于 1 的元素的阶为 2 或 4. 如果有一个元素的阶为 4，则 G 是循环群. 否则，对一切 $x \in G, x^2 = 1$，由习题 2.26，G 是阿贝尔群.

如果 x 和 y 是 G 中两个不等于 1 的不同元素，则立刻可验证 $xy \notin \{1, x, y\}$，因此

$$G = \{1, x, y, xy\}.$$

易知，由 $f(1) = 1, f(x) = (1\ 2)(3\ 4), f(y) = (1\ 3)(2\ 4)$ 和 $f(xy) = (1\ 4)(2\ 3)$ 定义的双射 $f: G \to \mathbf{V}$ 是同构.

在例 2.54 中已知$\mathbb{I}_4 \ncong \mathbf{V}$. ■ 97

命题 2.90 *如果 G 是 6 阶群，则 G 或者同构于$\mathbb{I}_6$，或者同构于 S_3. 此外，$\mathbb{I}_6$ 和 S_3 不同构*[㊀].

证明 由拉格朗日定理，非幺元元素可能的阶是 2，3，6. 当然，如果 G 有 6 阶元素，则$G \cong \mathbb{I}_6$. 习题 2.27 证明 G 必包含 2 阶元素，比如 t. 现在考虑 G 是阿贝尔群和非阿贝尔群两种情形.

第一种情形：G 是阿贝尔群.

如果有第二个 2 阶元素，比如 a，则由 $at = ta$ 易知 $H = \{1, a, t, at\}$ 是 G 的子群. 因 4 不是 6 的因数，所以这与拉格朗日定理矛盾. 由此 G 必含 3 阶元素 b，但由命题 2.82 知，tb 的阶为 6，所以如果 G 是阿贝尔群，则 G 必是循环群.

第二种情形：G 不是阿贝尔群.

如果 G 没有 3 阶元素，则对一切 $x \in G$，$x^2 = 1$，由习题 2.26 知 G 是阿贝尔群. 所以 G 包含 3 阶元素 s，同时还含有 2 阶元素 t.

现在 $|\langle s \rangle| = 3$，由此 $[G : \langle s \rangle] = |G| / |\langle s \rangle| = 6/3 = 2$. 根据命题 2.62（ii），$\langle s \rangle$是 G 的正规子群. 因 $t = t^{-1}$，所以有 $tst \in \langle s \rangle$，因此 $tst = s^i, i = 0, 1$ 或 2. 因 $tst = s^0 = 1$ 蕴涵 $s=1$，所以 $i \neq 0$. 如果 $i=1$，则 s 和 t 可交换，如同第一种情形那样可得 6 阶 st（因此 G 必是循环群，从而是阿贝尔群，这与现在的假设矛盾），所以 $tst = s^2 = s^{-1}$.

现在用定理 2.88 构造同构 $G \to S_3$. 令 $H = \langle t \rangle$，考虑由

$$\varphi(g) : x\langle t \rangle \mapsto gx\langle t \rangle$$

给出的同态 $\varphi: G \to S_{G/\langle t \rangle}$. 由定理知 $\ker\varphi \leqslant \langle t \rangle$，因此要么 $\ker\varphi = \{1\}$（从而 φ 是单射），要么 $\ker\varphi = \langle t \rangle$. 现在 $G/\langle t \rangle = \{\langle t \rangle, s\langle t \rangle, s^2\langle t \rangle\}$，排成两行的表示法是

$$\varphi(t) = \begin{pmatrix} \langle t \rangle & s\langle t \rangle & s^2\langle t \rangle \\ t\langle t \rangle & ts\langle t \rangle & ts^2\langle t \rangle \end{pmatrix}.$$

如果 $\varphi(t)$ 是恒等置换，则 $ts\langle t \rangle = s\langle t \rangle$，根据引理 2.40，$s^{-1}ts \in \langle t \rangle = \{1, t\}$. 但 $s^{-1}ts = t$（它不可能等于 1），因此 $ts = st$，这与 t 和 s 不交换相矛盾. 所以 $t \notin \ker\varphi$ 且 $\varphi: G \to S_{G/\langle t \rangle} \cong S_3$ 是单同态. 因 G 和 S_3 的阶都为 6，所以 φ 必是双射，从而 $G \cong S_3$.

㊀ 1854 年凯莱在一篇论文中叙述了这个命题，然而，1878 年，他在 American Journal of Mathematics 上写道："一般的问题是给定 n，求一切 n 阶群；…如果 $n=6$，则有三个群，一个是

$$1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5 \ (\alpha^6 = 1),$$

另两个形如

$$1, \beta, \beta^2, \alpha, \alpha\beta, \alpha\beta^2 \quad (\alpha^2 = 1, \beta^3 = 1),$$

在一个中 $\alpha\beta = \beta\alpha$，在另一个中 $\alpha\beta = \beta^2\alpha, \alpha\beta^2 = \beta\alpha$". 凯莱列出的是$\mathbb{I}_6$，$\mathbb{I}_2 \times \mathbb{I}_3$ 和 S_3，当然，$\mathbb{I}_2 \times \mathbb{I}_3 \cong \mathbb{I}_6$. 智者千虑，必有一失.

98 显然$\mathbb{I}_6$ 和 S_3 不同构，因为一个是阿贝尔群而另一个不是. ■

该结果的一个推论是给出了$\mathbb{I}_6 \cong \mathbb{I}_2 \times \mathbb{I}_3$ 的另一个证明(见定理 2.81).

由于我们尚未将理论展开到足够的程度，因此 8 阶群的分类更加困难. 已有的结果是 8 阶群，有 5 个不同构的群，其中三个是阿贝尔群：$\mathbb{I}_8$；$\mathbb{I}_4 \times \mathbb{I}_2$；$\mathbb{I}_2 \times \mathbb{I}_2 \times \mathbb{I}_2$；两个是非阿贝尔群：$D_8$；$\mathbf{Q}$.

对更大的阶可继续进行讨论，但很快会变得无法掌握，如表 2.4 所示. 做成群的电话号码簿不是研究它们的方法.

表 2.4

群的阶	群的数目
2	1
4	2
8	5
16	14
32	51
64	267
128	2 328
256	56 092
512	10 494 213
1024	49 487 365 422

群由置换的基本性质抽象而得，但置换的一个重要特征未被公理提及：置换是函数. 当恢复这个特征的时候，会得到重要的推论.

定义 设 X 是集合，G 是群. 如果有函数 $G \times X \to X$（记为 $(g,x) \mapsto gx$）使得

（ⅰ）对一切 g，$h \in G$ 和 $x \in X$，$(gh)x = g(hx)$；

（ⅱ）对一切 $x \in X$，$1x = x$，其中 1 是 G 的幺元.

则称为 G 作用在 X 上. 如果 G 作用在 X 上，也称 X 为 G-集.

如果群 G 作用在集合 X 上，则固定第一个变量，比如 g，给出函数 $\alpha_g: X \to X$，即 $\alpha_g: x \mapsto gx$. 该函数是 X 的一个置换，因为它的逆是 $\alpha_{g^{-1}}$：

$$\alpha_g \alpha_{g^{-1}} = \alpha_1 = 1_X = \alpha_{g^{-1}} \alpha_g.$$

易知，由 $\alpha: g \mapsto \alpha_g$ 定义的$\alpha: G \to S_X$ 是同态. 反之，给定同态 $\varphi: G \to S_X$，定义 $gx = \varphi(g)(x)$. 于是群 G 在集合 X 上的作用是用另一种方式来观察同态 $G \to S_X$.

凯莱定理说的是群 G 由（左）平移作用在它自身上，凯莱定理的推广，即定理 2.88 表明群 G 99 由（左）平移作用在它的子群 H 的陪集族上.

例 2.91 我们证明 G 由共轭作用在它自身上，即对每个 $g \in G$，定义 $\alpha_g: G \to G$ 为共轭

$$\alpha_g(x) = gxg^{-1}.$$

为验证公理（ⅰ），注意到对每个 $x \in G$，

$$\begin{aligned}(\alpha_g \circ \alpha_h)(x) &= \alpha_g(\alpha_h(x)) \\ &= \alpha_g(hxh^{-1}) \\ &= g(hxh^{-1})g^{-1} \\ &= (gh)x(gh)^{-1} \\ &= \alpha_{gh}(x).\end{aligned}$$

所以 $\alpha_g \circ \alpha_h = \alpha_{gh}$.

为证明公理（ⅱ），注意到对每个 $x\in G$，

$$\alpha_1(x)=1x1^{-1}=x,$$

由此 $\alpha_1=1_G$. ■

下面两个定义是基本的.

定义 如果 G 作用在 X 上且 $x\in X$，则 x 的**轨道**（记为 $\mathcal{O}(x)$）是指 X 的子集

$$\mathcal{O}(x)=\{gx: g\in G\}\subseteq X;$$

x 的**稳定化子**（记为 G_x）是指子群

$$G_x=\{g\in G: gx=x\}\leqslant G.$$

如果 G 作用在集合 X 上，定义 X 上的关系为 $x\equiv y$，如果存在 $g\in G$ 使得 $y=gx$. 易知它是等价关系，其等价类是轨道.

我们来求某些轨道和稳定化子.

例 2.92 （ⅰ）凯莱定理说群 G 由平移作用在它自身上：$\tau_g: a\mapsto ga$. 如果 $a\in G$，则轨道 $\mathcal{O}(a)=G$，因为如果 $b\in G$，则 $b=(ba^{-1})a=\tau_{ba^{-1}}(a)$. $a\in G$ 的稳定化子 G_a 是 $\{1\}$，因为如果 $a=\tau_g(a)=ga$，则 $g=1$. 称 G **传递地**作用在 X 上，如果只有一个轨道.

（ⅱ）当 G 由平移 $\tau_g: aH\mapsto gaH$ 作用在 G/H（子群 H 的陪集族）上时，轨道 $\mathcal{O}(aH)=G/H$，因为如果 $bH\in G/H$，则 $\tau_{ba^{-1}}: aH\mapsto bH$. 由此 G 传递地作用在 G/H 上. aH 的稳定化子 G_{aH} 是 aHa^{-1}，因为 $gaH=aH$ 当且仅当 $a^{-1}ga\in H$ 当且仅当 $g\in aHa^{-1}$. ■ [100]

例 2.93 当群 G 由共轭作用在自身上时，轨道 $\mathcal{O}(x)$ 是

$$\{y\in G: \text{有某个 } a\in G \text{ 使得 } y=axa^{-1}\}.$$

此时，称 $\mathcal{O}(x)$ 为 x 的**共轭类**，通常记为 x^G. 例如，定理 2.9 表明，如果 $\alpha\in S_n$，则 α 的共轭类由 S_n 中一切与 α 有同样轮换结构的置换组成. 作为第二个例子，元素 z 位于中心 $Z(G)$ 当且仅当 $z^G=\{z\}$，即 G 中没有其他元素与 z 共轭.

如果 $x\in G$，则 x 的稳定化子 G_x 是

$$C_G(x)=\{g\in G: gxg^{-1}=x\}.$$

G 的这个子群是由一切与 x 交换的 $g\in G$ 组成的，叫做 G 中 x 的**中心化子**. ■

例 2.94 每个群 G 由共轭作用在它的全体子群的集合 X 上：如果 $a\in G$，则 a 的作用是 $H\mapsto aHa^{-1}$，其中 $H\leqslant G$.

如果 H 是群 G 的子群，则 H 的**共轭**是 G 的形如

$$aHa^{-1}=\{aha^{-1}: h\in H\},$$

的子群，其中 $a\in G$.

因共轭 $h\mapsto aha^{-1}$ 是单射 $H\to G$，象为 aHa^{-1}，从而 G 的共轭子群是同构的. 例如在 S_3 中，一切 2 阶循环子群共轭(因为它们的生成元共轭).

子群 H 的轨道由它的一切共轭组成. 注意 H 的轨道中只有 H 一个元素当且仅当 $H\lhd G$；即对于一切 $a\in G$，$aHa^{-1}=H$. H 的稳定化子是

$$N_G(H)=\{g\in G: gHg^{-1}=H\}.$$

G 的这个子群叫做 G 中 H 的**正规化子**. ■

例 2.95 设 $X=$ 正方形顶点 $\{v_1, v_2, v_3, v_4\}$，又设作用在 X 上的群 G 是二面体群 D_8，如图 2.8（为清楚起见，图中顶点标以 1，2，3，4 以代替 v_1，v_2，v_3，v_4).

$$G = \{\text{旋转}:(1),(1\ 2\ 3\ 4),(1\ 3)(2\ 4),(1\ 4\ 3\ 2);$$
$$\text{反射}:(2\ 4),(1\ 3),(1\ 2)(3\ 4),(1\ 4)(2\ 3)\}.$$

对每个顶点 $v_i \in X$，有某个 $g \in G$ 使得 $gv_1 = v_i$，所以 $\mathcal{O}(v_1) = X$ 且 D_8 的作用是传递的.

v_1 的稳定化子 G_{V_1} 是什么？除了幺元外只有一个元素 $g \in D_8$ 固定 v_1，它就是 $g=(2\ 4)$，所以 101 G_{V_1} 是 2 阶子群(此例可推广到作用在正 n 边形上的二面体群 D_{2n}).

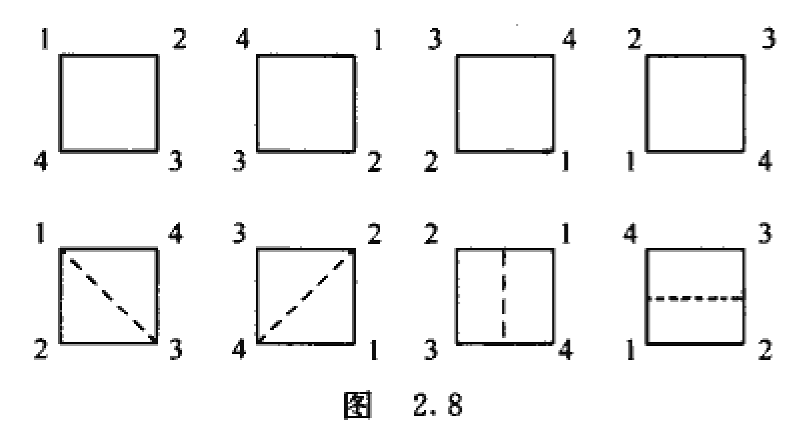


图 2.8

■

例 2.96 设 $X = \{1,2,\cdots,n\}$，$\alpha \in S_n$，并把循环群 $G=\langle\alpha\rangle$ 看作 X 上的作用. 如果 $i \in X$，则

$$\mathcal{O}(i) = \{\alpha^k(i) : k \in \mathbb{Z}\}.$$

设 $\alpha=\beta_1\cdots\beta_{t(\alpha)}$ 是 α 的完全轮换分解，并设 $i=i_1$ 被 α 移动. 如果包含 i_1 的轮换是 $\beta_j=(i_1 i_2 \cdots i_r)$，则定理 2.3 的证明表明对一切 $k<r$，$i_{k+1}=\alpha^k(i_1)$，所以

$$\mathcal{O}(i) = \{i_1, i_2, \cdots, i_r\},$$

其中 $i=i_1$. 由此 $|\mathcal{O}(i)|=r$. 如果 α 固定 ℓ，则数 ℓ 的稳定化子 G_ℓ 是 G. 然而，如果 α 移动 ℓ，则 G_ℓ 依赖于轨道 $\mathcal{O}(\ell)$ 的大小. 例如，$\alpha=(1\ 2\ 3)(4\ 5)(6)$，则 $G_6=G$，$G_1=\langle\alpha^3\rangle$，$G_4=\langle\alpha^2\rangle$. ■

命题 2.97 如果 G 作用在集合 X 上，则 X 是轨道的不相交并. 如果 X 是有限的，则

$$|X| = \sum_i |\mathcal{O}(x_i)|,$$

其中从每个轨道选取一个 x_i.

证明 早先已经提及，X 上的关系 $x \equiv y$（如果存在 $g \in G$ 使得 $y=gx$）是等价关系，它的等价类是轨道，所以轨道划分 X.

因轨道不相交，所以没有一个 X 的元素被计算两次，这样在第二个陈述中给出的计数结果是正确的. ■

下面是轨道和稳定化子之间的联系.

定理 2.98 如果 G 作用在集合 X 上且 $x \in X$，则

$$|\mathcal{O}(x)| = [G : G_x]$$

102 是 G 中稳定化子 G_x 的指数.

证明 令 G/G_x 为 G 中 G_x 的一切左陪集的族. 我们要举出一个双射：$\varphi: G/G_x \to \mathcal{O}(x)$，由此即可推出结论，这是因为 $|G/G_x| = [G : G_x]$. 定义 $\varphi: gG_x \mapsto gx$，现在 φ 是合理定义的：如果 $gG_x = hG_x$，则有某个 $f \in G_x$（即 $fx=x$）使得 $h=gf$. 因此，$hx=gfx=gx$. φ 是单射：如果 $gx = \varphi(gG_x) = \varphi(hG_x) = hx$，则 $h^{-1}gx=x$，因此 $h^{-1}g \in G_x$，从而 $gG_x = hG_x$. 最后，φ 是满射：如果 $y \in \mathcal{O}(x)$，则有某个 $g \in G$ 使得 $y=gx$，从而 $y=\varphi(gG_x)$. ■

在例 2.95 中，D_8 作用在正方形的四角上，我们看到 $|\mathcal{O}(v_1)|=4$，$|G_{v_1}|=2$ 和 $[G : G_{v_1}]=$

$8/2=4$. 在例 2.96 中，$G=\langle\alpha\rangle\leqslant S_n$ 作用在 $X=\{1,2,\cdots,n\}$ 上，我们看到如果在 α 分解为不相交轮换 $\alpha=\beta_1\cdots\beta_{t(\alpha)}$ 的完全轮换分解中，r-轮换 β_j 移动 ℓ，则对 β_j 包含的任一 ℓ，$r=|\mathcal{O}(\ell)|$. 定理 2.98 说 r 是 α 的阶 k 的因数(但定理 2.25 包含更多信息：k 是包含在轮换分解中的那些轮换的长度的 lcm).

系 2.99 如果有限群 G 作用在集合 X 上，则任一轨道中元素的个数是 $|G|$ 的因数.

证明 由拉格朗日定理立即可得. ■

在例2.5(ⅰ)中，有一个表格展示了 S_4 中每一种轮换结构的置换个数，它们是 1，6，8，6，3，注意这些数都是 $|S_4|=24$ 的因数. 在例2.5(ⅱ)中，我们看到相应的数目是 1，10，20，30，24，20，15，这些数都是 $|S_5|=120$ 的因数. 现在我们已经认识了这些子集是共轭类. 下一个系解释为什么这些数整除群的阶.

系 2.100 如果 x 在有限群 G 中，则 x 的共轭的个数是它的中心化子的指数：

$$|x^G|=[G:C_G(x)],$$

因此它是 $|G|$ 的因数.

证明 如同例 2.93，x 的轨道是它的共轭类 x^G，稳定化子 G_x 是中心化子 $G_G(x)$. ■

命题 2.101 设 H 是有限群 G 的子群，则 G 中 H 的共轭的个数是 $[G:N_G(H)]$.

证明 如同例 2.94，H 的轨道是它的一切共轭的族，而稳定化子是它的正规化子 $N_G(H)$. ■

群的作用在计数问题中有一些重要的应用，本节末尾将给出这种应用，现在我们先把群的作用应用到群论上.

当我们开始对 6 阶群分类的时候，如果能够断定任一 6 阶群都有一个 3 阶元素将是很有帮助的(较早的习题已经断定 2 阶元素的存在). 现在证明如果 p 是 $|G|$ 的素因数，其中 G 是一个有限群，则 G 包含 p 阶元素.

103

定理 2.102 (柯西) 如果 G 是有限群，它的阶被素数 p 整除，则 G 含有 p 阶元素.

证明 对 $m\geqslant 1$ 用归纳法证明该定理，其中 $|G|=pm$. 因拉格朗日定理证明在 p 阶群中，每个非幺元元素的阶都是 p，所以基础步 $m=1$ 为真.

现在证明归纳步. 如果 $x\in G$，则 x 的共轭的个数是 $|x^G|=[G:C_G(x)]$，其中 $C_G(x)$ 是 x 在 G 中的中心化子. 早先已经指出，如果 $x\notin Z(G)$，则 x^G 的元素多于一个，因此 $|C_G(x)|<|G|$. 如果对某个非中心的 x，$p\mid|C_G(x)|$，则归纳假设说在 $C_G(x)\leqslant G$ 中有 p 阶元素，结果已经得到. 所以可假定对一切非中心的 $x\in G$，$p\nmid|C_G(x)|$. 因 p 是素数且 $|G|=[G:C_G(x)]|C_G(x)|$，欧几里得引理给出

$$p\mid[G:C_G(x)].$$

回顾 $Z(G)$ 由一切满足 $|x^G|=1$ 的元素 $x\in G$ 组成，由命题 2.97 可知

$$|G|=|Z(G)|+\sum_i[G:C_G(x_i)],$$

其中在每个多于一个元素的共轭类中取出一个 x_i. 因 $|G|$ 和所有 $[G:C_G(x)]$ 都被 p 整除，从而 $|Z(G)|$ 被 p 整除. 但 $Z(G)$ 是阿贝尔群，因此命题 2.78 说 $Z(G)$ (从而 G) 包含 p 阶元素. ■

定义 有限群 G 的**类方程**是指

$$|G|=|Z(G)|+\sum_i[G:C_G(x_i)],$$

其中在每个多于一个元素的共轭类中取出一个元素 x_i.

定义 假定 p 是素数，则有限群 G 称为 p-群，如果有某个 $n\geqslant 0$ 使得 $|G|=p^n$.（关于无限 p-群的定义见习题 2.81.）

我们已经见过中心平凡的群的例子，例如，$Z(S_3)=\{1\}$. 然而，对于 p-群永远不可能出现这种情形.

定理 2.103 如果 p 是素数，$G\neq\{1\}$ 是 p-群，则 $Z(G)\neq\{1\}$.

证明 考虑类方程

$$|G|=|Z(G)|+\sum_i[G:C_G(x_i)].$$

对于 $x_i\notin Z(G)$，每个 $C_G(x_i)$ 是 G 的真子群. 由于 G 是 p-群，则 $[G:C_G(x_i)]$ 是 $|G|$ 的因数，因此它也是 p 的幂. 于是 p 整除类方程中除 $|Z(G)|$ 外的每一项，从而 $p\mid|Z(G)|$，所以 $Z(G)\neq$ 104 $\{1\}$. ■

系 2.104 如果 p 是素数，则每个阶为 p^2 的群都是阿贝尔群.

证明 如果 G 不是阿贝尔群，则它的中心 $Z(G)$ 是真子群，于是由拉格朗日定理，$|Z(G)|=1$ 或 p. 但定理 2.103 说 $Z(G)\neq\{1\}$，因此 $|Z(G)|=p$. 中心恒为正规子群，从而商群 $G/Z(G)$ 是有定义的，它的阶为 p，于是 $G/Z(G)$ 是循环群，这与习题 2.69 矛盾. ■

例 2.105 谁会想到柯西定理（如果 G 是群，它的阶为素数 p 的倍数，则 G 有 p 阶元素）和费马定理（如果 p 是素数，则 $a^p\equiv a\bmod p$）都是一个普遍定理的特殊情形？柯西定理的一个初等的但有独创性的证明属于 J. H. Mckay，1959 年（见 Montgomery 和 Ralston 所著的《Selected Papers in Algebra》）. A. Mann 告诉我 Mckay 的论证也证明了费马定理. 如果 G 是有限群，p 是素数，则记 p 个 G 的笛卡儿积为 G^p，且定义

$$X=\{(a_0,a_1,\cdots,a_{p-1})\in G^p:a_0a_1\cdots a_{p-1}=1\}.$$

注意 $|X|=|G|^{p-1}$，这是因为任意选定了后面 $p-1$ 个元素之后，第 0 个元素必等于 $(a_1a_2\cdots a_{p-1})^{-1}$. 引入 $\mathbb{I}_p$ 在 X 上的作用，定义为：对 $0\leqslant i\leqslant p-1$，

$$[i](a_0,a_1,\cdots,a_{p-1})=(a_i,a_{i+1},\cdots,a_{p-1},a_0,a_1,\cdots,a_{i-1}).$$

新的 p 元组中的元素之积是 $a_0a_1\cdots a_{p-1}$ 的共轭：

$$a_ia_{i+1}\cdots a_{p-1}a_0a_1\cdots a_{i-1}=(a_0a_1\cdots a_{i-1})^{-1}(a_0a_1\cdots a_{p-1})(a_0a_1\cdots a_{i-1}).$$

这个共轭是 1（因为 $g^{-1}1g=1$），因此 $[i](a_0,a_1,\cdots,a_{p-1})\in X$. 由系 2.99，$X$ 的每个轨道的大小是 $|\mathbb{I}_p|=p$ 的因数，因 p 是素数，该轨道的大小或者是 1，或者是 p. 现在 p 元组的每个元素 a_i 都相等，p 元组构成的轨道只含一个元素，这是因为 p 元组的所有循环置换都是一样的. 换句话说，这样的轨道对应于满足 $a^p=1$ 的元素 $a\in G$. 显然，$(1,1,\cdots,1)$ 是这样的轨道. 如果这样的轨道只有这一个，则有某个 $k\geqslant 0$ 使得

$$|G|^{p-1}=|X|=1+kp.$$

即 $|G|^{p-1}\equiv 1\bmod p$. 如果 p 是 $|G|$ 的因数，则 $|G|^{p-1}\equiv 0\bmod p$，于是产生矛盾. 由此已经证明了柯西定理：如果素数 p 是 $|G|$ 的因数，则 G 有 p 阶元素.

现在假设 G 是 n 阶群，比如 $G=\mathbb{I}_n$，且 p 不是 n 的因数. 由拉格朗日定理，G 没有 p 阶元素，于是，如果 $a^p=1$，则 $a=1$. 所以 G^p 中大小为 1 的唯一轨道是 $(1,1,\cdots,1)$，由此，

$$n^{p-1}=|G|^{p-1}=|X|=1+kp;$$

即如果 p 不是 n 的因数，则 $n^{p-1}\equiv 1\bmod p$，两端同乘 n 得 $n^p\equiv n\bmod p$. 当 p 是 n 的因数时，该同 105 余式仍然成立，这就是费马定理. ■

在命题 2.64 中已经看到 A_4 是 12 阶群，它没有 6 阶子群，由此下面的论断是错误的：如果 d 是 $|G|$ 的因数，则 G 必有 d 阶子群．然而当 G 是 p-群时，该结论成立．

命题 2.106 如果 G 是群，其阶 $|G|=p^e$，则对每个 $k\leqslant e$，G 有 p^k 阶正规子群．

证明 对 $e\geqslant 0$ 用归纳法证明该结果．基础步显然成立，因而进入归纳步．由定理 2.103，G 的中心是非平凡的正规子群：$Z(G)\neq\{1\}$．令 $Z\leqslant Z(G)$ 是 p 阶子群，因为 Z 是 $Z(G)$ 的任一子群，所以子群 Z 是 G 的正规子群．如果 $k\leqslant e$，则 $p^{k-1}\leqslant p^{e-1}=|G/Z|$．由归纳假设，$G/Z$ 有 p^{k-1} 阶正规子群 H^*．对应的定理说，有 G 的包含 Z 的子群 H 使得 $H^*=H/Z$．此外，$H^*\lhd G/Z$ 蕴涵 $H\lhd G$，但 $|H/Z|=p^{k-1}$ 蕴涵要证明的结果 $|H|=p^k$． ■

阿贝尔群(和四元数)有一个性质，就是每个子群都是正规子群．与之相对的是这样的群，就是除了两个明显的子群 $\{1\}$ 和 G 之外没有其他任何正规子群．

定义 群 G 称为**单群**，如果 $G\neq\{1\}$ 且除了 $\{1\}$ 和 G 自身外没有其他任何正规子群．

定理 2.107 阿贝尔群 G 是单群当且仅当它是有限的，且阶为素数．

证明 如果 G 是阶为素数 p 的有限群，则除了 $\{1\}$ 和 G 之外，G 没有别的子群 H，否则，拉格朗日定理将证明 $|H|$ 是 p 的因数．所以 G 是单群．

反之，假定 G 是单群．因 G 是阿贝尔群，所以每个子群都是正规子群，从而除了 $\{1\}$ 和 G 之外，G 没有别的子群．选取 $x\in G$ 且 $x\neq 1$，因 $\langle x\rangle$ 是一个子群，所以 $\langle x\rangle=G$．如果 x 的阶无限，则 x 所有的幂都不同，于是 $\langle x^2\rangle<\langle x\rangle$ 是一个不允许存在的子群，从而产生矛盾．因此每个 $x\in G$ 的阶有限．如果 x 的阶为 m（有限)，且 m 为合数，比如 $m=k\ell$，则 $\langle x^k\rangle$ 是 $\langle x\rangle$ 的一个非平凡的真子群，这就产生矛盾．所以 $G=\langle x\rangle$ 的阶为素数． ■

现在证明 A_5 是一个非阿贝尔的单群(其实它是这种群中最小的一个，没有阶小于 60 的非阿贝尔单群)．

假设元素 $x\in G$ 有 k 个共轭，即

$$|x^G|=|\{gxg^{-1}:g\in G\}|=k.$$

如果有子群 $H\leqslant G$ 满足 $x\in H\leqslant G$，则 x 在 H 中有多少个共轭？因

$$x^H=\{hxh^{-1}:h\in H\}\subseteq\{gxg^{-1}:g\in G\}=x^G,$$

[106]

所以有 $|x^H|\leqslant|x^G|$．严格的不等式 $|x^H|<|x^G|$ 有可能成立．例如，取 $G=S_3, x=(1\ 2)$，$H=\langle x\rangle$，我们知道 $|x^G|=3$（因为所有对换都是共轭的)，而 $|x^H|=1$（因为 H 是阿贝尔群)．

现在特别考虑 $G=S_5, x=(1\ 2\ 3), H=A_5$ 的情形．

引理 2.108 在 A_5 中一切 3-轮换都是共轭的．

证明 设 $G=S_5$，$\alpha=(1\ 2\ 3)$，$H=A_5$．在例2.5(ii) 中已知 S_5 中有 20 个 3-轮换，因此 $|\alpha^{S_5}|=20$．由系 2.100，$20=|S_5|/|C_{S_5}(\alpha)|=120/|C_{S_5}(\alpha)|$，从而 $|C_{S_5}(\alpha)|=6$，即 S_5 中恰有 6 个置换与 α 可交换，它们是

$$(1),(1\ 2\ 3),(1\ 3\ 2),(4\ 5),(4\ 5)(1\ 2\ 3),(4\ 5)(1\ 3\ 2).$$

后三个是奇置换，因此 $|C_{A_5}(\alpha)|=3$，由此可知

$$|\alpha^{A_5}|=|A_5|/|C_{A_5}(\alpha)|=60/3=20;$$

即 A_5 中所有 3-轮换都与 $\alpha=(1\ 2\ 3)$ 共轭． ■

这个引理可从 A_5 推广到 $n\geqslant 5$ 的所有 A_n，见习题 2.91．

引理 2.109 如果 $n\geqslant 3$，则 A_n 的每个元素不是一个 3-轮换就是 3-轮换的乘积.

证明 如果 $\alpha\in A_n$，则 α 是偶数个对换的乘积：

$$\alpha=\tau_1\tau_2\cdots\tau_{2q-1}\tau_{2q}.$$

当然可假设相邻的那些 τ 是不同的. 因为可把这些对换配成 $\tau_{2i-1}\tau_{2i}$ 为一对，只需考虑 $\tau\tau'$，其中 τ 和 τ'是对换. 如果 τ 和 τ'相交，则 $\tau=(i\ j)$，$\tau'=(i\ k)$，且 $\tau\tau'=(i\ k\ j)$；如果 τ 和 τ'不相交，则 $\tau\tau'=(i\ j)(k\ \ell)=(i\ j)(j\ k)(j\ k)(k\ \ell)=(i\ j\ k)(j\ k\ \ell)$. ■

定理 2.110 A_5 是单群.

证明 我们将证明：如果 H 是 A_5 的正规子群，且 $H\neq\{(1)\}$，则 $H=A_5$. 现在，如果 H 含有一个 3-轮换，则正规性迫使 H 包含它的一切共轭. 由引理 2.108，H 包含每个 3-轮换，再由引理 2.109，$H=A_5$. 所以只需证明 H 含有一个 3-轮换.

因为 $H\neq\{(1)\}$，所以 H 包含某个 $\sigma\neq(1)$. 在不失一般性地重新标号后，可假设或者$\sigma=(1\ 2\ 3)$，或者$\sigma=(1\ 2)(3\ 4)$，或者 $\sigma=(1\ 2\ 3\ 4\ 5)$. 刚才已说明，如果 σ 是 3-轮换，证明便完成.

如果 $\sigma=(1\ 2)(3\ 4)$，定义 $\tau=(1\ 2)(3\ 5)$. 现在，因 H 是正规子群，所以 H 包含 $(\tau\sigma\tau^{-1})\sigma^{-1}$，读者可验证 $\tau\sigma\tau^{-1}\sigma^{-1}=(3\ 5\ 4)$. 如果 $\sigma=(1\ 2\ 3\ 4\ 5)$，定义 $\rho=(1\ 3\ 2)$. 现在 H 包含 $\rho\sigma\rho^{-1}\sigma^{-1}$，读者可验证 $\rho\sigma\rho^{-1}\sigma^{-1}=(1\ 3\ 4)$.

上面证明了在所有情形中，H 都含有 3-轮换，所以 A_5 中只有 $\{(1)\}$ 和 A_5 自身两个正规子群，从而 A_5 是单群. ■

107

定理 2.110 给出了四次公式没有推广为 5 次或高次多项式的求根公式的基本理由（见定理 4.27).

不用花很多精力，就可证明对于一切 $n\geqslant 5$，交错群 A_n 都是单群. 可以看到 A_4 不是单群，因为四群 $\mathbf{V}$ 不是 A_4 的正规子群.

引理 2.111 A_6 是单群.

证明 设 $H\neq\{(1)\}$ 是 A_6 的正规子群，我们需要证明 $H=A_6$. 假定有某个 $\alpha\in H$ 满足$\alpha\neq(1)$且固定某个 i，其中 $1\leqslant i\leqslant 6$. 定义

$$F=\{\sigma\in A_6:\sigma(i)=i\}.$$

注意 $\alpha\in H\cap F$，从而 $H\cap F\neq\{(1)\}$. 第二同构定理给出 $H\cap F\lhd F$. 因 $F\cong A_5$，所以 F 是单群，从而 F 中的正规子群只有$\{(1)\}$和 F. 因 $H\cap F\neq\{(1)\}$，所以有 $H\cap F=F$，即 $F\leqslant H$. 由此导出 H 含有 3-轮换，从而由习题 2.91，$H=A_6$.

现在可假设不存在 $\alpha\in H$ 满足 $\alpha\neq(1)$且固定某个 i，其中 $1\leqslant i\leqslant 6$. 考虑 A_6 中的置换的轮换结构，任何这样的 α 必有轮换结构$(1\ 2)(3\ 4\ 5\ 6)$或$(1\ 2\ 3)(4\ 5\ 6)$. 在第一种情形中，$\alpha^2\in H$ 是非平凡置换，它固定 1(还有 2)，这便产生矛盾. 在第二种情形中，H 包含 $\alpha(\beta\alpha^{-1}\beta^{-1})$，其中$\beta=(2\ 3\ 4)$，容易验证它是 H 中固定 1 的一个非平凡元素，于是又产生矛盾. 所以这样的正规子群不存在，从而 A_6 是单群. ■

定理 2.112 对一切 $n\geqslant 5$，A_n 是单群.

证明 如果 H 是 A_n 的非平凡的正规子群，即$H\neq\{(1)\}$，则我们必须证明 $H=A_n$. 由习题 2.91，只需证明 H 含有 3-轮换. 如果 $\beta\in H$ 是非平凡的，则有某个 i 被 β 移动，比如 $\beta(i)=j\neq i$. 选取一个 3-轮换 α 固定 i 并移动 j. 置换 α 和 β 不交换：$\beta\alpha(i)=\beta(i)=j$，而 $\alpha\beta(i)=\alpha(j)\neq j$. 由此 $\gamma=(\alpha\beta\alpha^{-1})\beta^{-1}$ 是 H 中的非平凡元素. 但由定理 2.9，$\beta\alpha^{-1}\beta^{-1}$ 是 3-轮换，从而 $\gamma=\alpha(\beta\alpha^{-1}\beta^{-1})$ 是两个 3-轮换的积，于是 γ 最多移动 6 个符号，比如 $i_1,\cdots,i_6$（如果 γ 移动的符号少于 6 个，则把其他符号添

加到后面从而形成 6 个元素的表). 定义

$$F=\{\sigma\in A_n:\sigma\text{ 固定一切 } i\neq i_1,\cdots,i_6\}.$$

现在 $F\cong A_6$ 且 $\gamma\in H\cap F$，因此 $H\cap F$ 是 F 的非平凡正规子群. 但 F 是同构于 A_6 的单群，所以 $H\cap F=F$；即 $F\leqslant H$. 所以 H 含有 3-轮换，由此 $H=A_n$. 证明完成. ■

我们现在利用群来求解若干困难的计数问题. [108]

定理 2.113(伯恩赛德引理⊖) *设 G 是一个作用在有限集合 X 上的有限群，令 N 为轨道的个数，则*

$$N=\frac{1}{|G|}\sum_{\tau\in G}\mathrm{Fix}(\tau),$$

其中 $\mathrm{Fix}(\tau)$ 是被 τ 固定的 $x\in X$ 的个数.

证明 把 X 的元素列表如下：选取 $x_1\in X$，然后列出轨道 $\mathcal{O}(x_1)$ 中所有的元素 x_1，x_2，…，x_r；再选取 $x_{r+1}\notin\mathcal{O}(x_1)$，列出 $\mathcal{O}(x_{r+1})$ 中所有的元素 x_{r+1}，x_{r+2}，…. 继续进行直到 X 的一切元素都列完. 现在列出 G 的元素 τ_1，τ_2，…，τ_n 并形成下面的阵列，其中

$$f_{i,j}=\begin{cases}1 & \text{如果 } \tau_i \text{ 固定 } x_j\\ 0 & \text{如果 } \tau_i \text{ 移动 } x_j\end{cases}$$

	x_1	x_2	…	x_{r+1}	x_{r+2}	…
τ_1	$f_{1,1}$	$f_{1,2}$	…	$f_{1,r+1}$	$f_{1,r+2}$	…
τ_2	$f_{2,1}$	$f_{2,2}$	…	$f_{2,r+1}$	$f_{2,r+2}$	…
τ_i	$f_{i,1}$	$f_{i,2}$	…	$f_{i,r+1}$	$f_{i,r+2}$	…
τ_n	$f_{n,1}$	$f_{n,2}$	…	$f_{n,r+1}$	$f_{n,r+2}$	…

现在被 τ_i 固定的 x 的个数 $\mathrm{Fix}(\tau_i)$ 是阵列第 i 行中 1 的个数，所以 $\sum_{\tau\in G}\mathrm{Fix}(\tau)$ 是阵列中 1 的总数. 再来看列，第一列中 1 的个数是固定 x_1 的 τ_i 的个数. 由定义，这些 τ_i 组成 G_{x_1}，于是第一列中 1 的个数是 $|G_{x_1}|$. 同样，第二列中 1 的个数是 $|G_{x_2}|$. 由习题 2.99，$|G_{x_1}|=|G_{x_2}|$. 根据定理 2.98，标以 $x_i\in\mathcal{O}(x_1)$ 的 r 个列中 1 的个数是

$$r|G_{x_1}|=|\mathcal{O}(x_1)|\cdot|G_{x_1}|=(|G|/|G_{x_1}|)|G_{x_1}|=|G|.$$

对其他轨道有相同的结果：每个轨道相应的列恰含 $|G|$ 个 1. 所以，如果有 N 个轨道，在阵列中就有 $N|G|$ 个 1. 由此可知

$$\sum_{\tau\in G}\mathrm{Fix}(\tau)=N|G|.$$ ■

现在用伯恩赛德引理来解下面类型的问题. 有六个条幅(等宽)，每个着以红色、白色或蓝色，把这些条幅连成一面长条旗，这种旗子有多少种？显然图 2.9 中所示的两种旗子是一样的：下面一种是上面一种的反转. [109]

⊖ 伯恩赛德自己把该引理归于弗罗贝尼乌斯(F. G. Frobenius). 为了避免因改换为普通名称而引起的混乱，诺伊曼(P. M. Neumann)曾建议称之为"非伯恩赛德引理". 伯恩赛德是优秀的数学家，有真正属于他的定理，例如，伯恩赛德证明：如果 p 和 q 是素数，则不存在 p^mq^n 阶单群.



图 2.9

设 X 为颜色的一切 6 元组的集合，如果 $x\in X$，则

$$x=(c_1,c_2,c_3,c_4,c_5,c_6),$$

其中每个 c_i 表示红色、白色或蓝色. 令 τ 为反转所有标号的置换：

$$\tau=\begin{pmatrix}1&2&3&4&5&6\\6&5&4&3&2&1\end{pmatrix}=(1\ 6)(2\ 5)(3\ 4)$$

(由此，τ "反转" 每个着色条幅的 6 元组). 循环群 $G=\langle\tau\rangle$作用在 X 上. 因 $|G|=2$，所以 6 元组 x 的轨道由 1 个或 2 个元素组成：τ 或者固定 x，或者不固定 x. 因反转后旗子是不变的，所以把旗子等同于 6 元组的轨道是合理的. 例如由 6 元组

(红,白,蓝,红,白,蓝) 和(蓝,白,红,蓝,白,红)

组成的轨道描述了图 2.9 中的旗子. 由此，旗子的数目就是轨道的数目 N，根据伯恩赛德引理，$N=\frac{1}{2}[\text{Fix}((1))+\text{Fix}(\tau)]$. 恒等置换 (1) 固定每个 $x\in X$，因此 $\text{Fix}((1))=3^6$ (有 3 种颜色). 如果 6 元组 x 是 "回文"，即 x 中的颜色顺读倒读都一样，则 τ 固定 x；例如 τ 固定

$x=$ (红,红,白,白,红,红).

反之，如果

$$x=(c_1,c_2,c_3,c_4,c_5,c_6)$$

被 $\tau=(1\ 6)(2\ 5)(3\ 4)$ 固定，则 $c_1=c_6$，$c_2=c_5$，$c_3=c_4$，即 x 是一个顺读倒读都一样的字. 由此，$\text{Fix}(\tau)=3^3$，这是因为 c_1，c_2，c_3 各有三种颜色. 于是旗子的数目为

$$N=\frac{1}{2}(3^6+3^3)=378.$$

下面我们把着色概念表述得更精确一些.

定义 *如果群 G 作用在 $X=\{1,2,\cdots,n\}$ 上，$\mathcal{C}$是 q 种颜色的集合，则 G 在颜色的一切 n 元组的集合$\mathcal{C}^n$ 上的作用为对一切 $\tau\in G$，*

$$\tau(c_1,\cdots,c_n)=(c_{\tau 1},\cdots,c_{\tau n}).$$

110 *称 $(c_1,\cdots,c_n)\in\mathcal{C}^n$ 的轨道为 X 的* **(q,G)-着色**.

例 2.114 给 4×4 网格的每个方块着以红色或黑色(相邻方块可以有相同的颜色，事实上，有一种可能是所有方块着同一颜色).

如果 X 由网格中的 16 个方块组成，$\mathcal{C}$由红、黑两种颜色组成，则 4 阶循环群 $G=\langle R\rangle$作用在 X 上，其中 R 是顺时针旋转 90°. 图 2.10 表示 R 是如何作用的：右边的正方形是 R 在左边正方形上的作用，用轮换记号来记是：

$$R=(1,4,16,13)(2,8,15,9)(3,12,14,5)(6,7,11,10),$$

$$R^2=(1,16)(4,13)(2,15)(8,9)(3,14)(12,5)(6,11)(7,10),$$

$$R^3=(1,13,16,4)(2,9,15,8)(3,5,14,12)(6,10,11,7).$$

旋转时，红黑相间的棋盘是不变的，只不过是从另一个角度来观察而已. 由此我们把一个棋盘看作是 X 的一个 2-着色. 一个 16 元组的轨道对应于观察一个棋盘的四个角度.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

13	9	5	1
14	10	6	2
15	11	7	3
16	12	8	4

图 2.10

由伯恩赛德引理，棋盘数是

$$\frac{1}{4}[\mathrm{Fix}((1)) + \mathrm{Fix}(R) + \mathrm{Fix}(R^2) + \mathrm{Fix}(R^3)].$$

现在 $\mathrm{Fix}((1)) = 2^{16}$，这是因为恒等置换固定每个 16 元组. 为计算 $\mathrm{Fix}(R)$，注意被 R 固定的 16 元组中，1，4，16，13 四个方块颜色必须相同. 同样，方块 2，8，15，9 颜色必须相同，方块 3，12，14，5 颜色必须相同，方块 6，7，11，10 颜色必须相同. 由此可知 $\mathrm{Fix}(R) = 2^4$. 注意指数 4 是 R 的完全轮换分解中轮换的个数. 类似的分析表明 $\mathrm{Fix}(R^2) = 2^8$，这是因为 R^2 的完全轮换分解中有 8 个轮换. $\mathrm{Fix}(R^3) = 2^4$，这是因为 R^3 的轮换结构和 R 的相同. 所以棋盘数 N 是

$$N = \frac{1}{4}[2^{16} + 2^4 + 2^8 + 2^4] = 16\,456.$$ ■ [111]

现在证明置换 τ 的轮换结构可用来计算 $\mathrm{Fix}(\tau)$，如例 2.114 那样.

引理 2.115 设$\mathcal{C}$是 q 种颜色的集合，G 是 S_n 的子群. 如果 $\tau \in G$，则

$$\mathrm{Fix}(\tau) = q^{t(\tau)},$$

其中 $t(\tau)$是 τ 的完全轮换分解中轮换的个数.

证明 因 $\tau(c_1, \cdots, c_n) = (c_{\tau 1}, \cdots, c_{\tau n}) = (c_1, \cdots, c_n)$，从而对一切 i 有 $c_{\tau i} = c_i$，即 τi 和 i 的颜色相同，由此对所有 k，$\tau^k i$ 和 i 的颜色相同，即在$\langle\tau\rangle$作用下，i 的轨道上一切点的颜色都相同. 如果 τ 的完全轮换分解是 $\tau = \beta_1 \cdots \beta_{t(\tau)}$，且 i 在β_j 中出现，则例 2.96 证明包含 i 的轨道是出现在β_j 中的符号的集合. 这样，因 n 元组被 τ 固定，所以 $t(\tau)$个轮换中的每一个所含的符号必有同一颜色，而颜色有 q 种，从而有 $q^{t(\tau)}$ 个 n 元组被 τ 固定. ■

系 2.116 设 G 作用在有限集 X 上. 令 N 为 X 的 (q, G)-着色的数目，则

$$N = \frac{1}{|G|}\sum_{\tau \in G} q^{t(\tau)},$$

其中 $t(\tau)$是 τ 的完全轮换分解中轮换的个数.

G. Pólya 推广了这个方法(见 Biggs 所著的《Discrete Mathematics》). 例如，他给出了下面这种旗子种数的计算公式：每个条幅有红、白、蓝、绿四种颜色，20 个条幅组成一面旗子，其中恰有 7 个条幅是红的，5 个条幅是蓝的.

习题

2.78 如果 a，b 是群 G 的元素，证明 ab 和 ba 的阶相同.
提示：用共轭.

2.79 如果 G 是奇数阶有限群，证明除 $x=1$ 之外没有元素和它的逆共轭.
提示：如果 x 和 x^{-1} 共轭，则 x^G 中有多少元素？

2.80　证明下列 8 阶群中没有一对同构：

$$\mathbb{I}_8;\mathbb{I}_4\times\mathbb{I}_2;\mathbb{I}_2\times\mathbb{I}_2\times\mathbb{I}_2;D_8;\mathbf{Q},$$

2.81　如果 p 是素数，G 是有限群，其元素的阶都是 p 的幂．证明 G 是 p-群（称无限群 G 为 p-群，如果 G 中元素的阶都是 p 的幂）．

112

提示：用柯西定理．

2.82　定义子群 $H\leqslant G$ 的**中心化子** $C_G(H)$ 为

$$C_G(H)=\{x\in G：对一切\ h\in H,xh=hx\}.$$

（ⅰ）对每个子群 $H\leqslant G$，证明 $C_G(H)\lhd N_G(H)$．

（ⅱ）对每个子群 $H\leqslant G$，证明 $N_G(H)/C_G(H)$ 同构于 $\mathrm{Aut}(H)$ 的一个子群．

提示：推广习题 2.64 中的同态 Γ．

2.83　证明 S_4 有一个子群与 D_8 同构．

2.84　证明 $S_4/\mathbf{V}\cong S_3$．

提示：用命题 2.90．

2.85　（ⅰ）证明 $A_4\ncong D_{12}$．

提示：回忆 A_4 没有 6 阶元素．

（ⅱ）证明 $D_{12}\cong S_3\times\mathbb{I}_2$．

提示：每个元素 $x\in D_{12}$ 可唯一地因子分解为 $x=b^ia$ 的形式，其中 $b^6=1$，$a^2=1$．

2.86　（ⅰ）假定 G 是群，则正规子群 $H\lhd G$ 称为**极大正规子群**，如果没有 G 的正规子群 K 满足 $H<K<G$．证明正规子群 H 是 G 的极大正规子群当且仅当 G/H 是单群．

（ⅱ）证明每个有限阿贝尔群 G 有指数为素数的子群．

提示：用命题 2.107．

（ⅲ）证明 A_6 没有指数为素数的子群．

2.87　证明 $H\lhd N_G(H)$，且 $N_G(H)$ 是 G 中包含 H 并把 H 作为正规子群的最大子群．

2.88　如果 $G=S_4$，$H=\langle(1\ 2\ 3)\rangle$，求 $N_G(H)$．

2.89　（ⅰ）如果 H 是 G 的子群且 $x\in H$．证明

$$C_H(x)=H\cap C_G(x).$$

（ⅱ）如果 H 是有限群 G 中指数为 2 的子群，且 $x\in H$，证明 $|x^H|=|x^G|$ 或 $|x^H|=\frac{1}{2}|x^G|$，其中 x^H 是 x 在 H 中的共轭类．

提示：用第二同构定理．

（ⅲ）证明在 A_5 中有两个 5-轮换的共轭类，每个有 12 个元素．

提示：如果 $\alpha=(1\ 2\ 3\ 4\ 5)$，则因 $24=\dfrac{120}{|C_{S_5}(\alpha)|}$，所以 $|C_{S_5}(\alpha)|=5$，由此 $C_{S_5}(\alpha)=\langle\alpha\rangle$．$C_{A_5}(\alpha)$ 是什么？

（ⅳ）证明 A_5 中共轭类的大小是 1，12，12，15，20．

2.90　（ⅰ）证明群 G 的每个正规子群 H 是 G 的共轭类的并，其中的一个共轭类是 $\{1\}$．

（ⅱ）用（ⅰ）和习题 2.89 给出 A_5 的单性的第二个证明．

2.91　（ⅰ）对一切 $n\geqslant5$，证明 A_n 中所有 3-轮换共轭．

提示：分两步证明（1 2 3）和（$i\ j\ k$）共轭：首先假定它们相交（由此，该两个置换最多移动 5 个字母）；然后假定它们不相交．

113

（ⅱ）证明：如果正规子群 $H\lhd A_n$ 包含 3-轮换，其中 $n\geqslant5$，则 $H=A_n$．

(注：引理 2.109 已证明了 $n=5$ 的情形.)

2.92 证明 S_4 的正规子群只有$\{(1)\}$，$\mathbf{V}$，A_4，S_4.

提示：用定理 2.9，检查各个轮换结构.

2.93 证明 60 阶群 A_5 没有 30 阶子群.

提示：用命题 2.62（ii）.

2.94 （i）对一切 $n\geqslant 5$，证明 S_n 的正规子群只有$\{(1)\}$，A_n 和 S_n.

（ii）对一切 $n\geqslant 3$，证明在 S_n 中，A_n 是唯一的阶为$\frac{1}{2}n!$ 的子群.

提示：如果 H 是第二个这样的子群，则 H 是 S_n 中的正规子群，因此 $H\cap A_n$ 是 A_n 中的正规子群.

（iii）证明 S_5 中没有 30 阶子群.

提示：假设有 30 阶子群，用陪集上的表示以及 A_5 的单性.

（iv）证明 S_5 不含 40 阶子群.

2.95 设 G 是 S_n 的子群.

（i）如果 $G\cap A_n=\{1\}$，证明 $|G|\leqslant 2$.

（ii）如果 G 是多于 2 个元素的单群，证明 $G\leqslant A_n$.

2.96 （i）如果 $n\geqslant 5$，证明 S_n 没有指数为 r 的子群，其中 $2<r<n$.

（ii）如果 $n\geqslant 5$，证明 A_n 没有指数为 r 的子群，其中 $2\leqslant r<n$.

2.97 （i）如果单群 G 有指数为 $n>1$ 的子群，证明 G 同构于 S_n 的一个子群.

提示：核是正规子群.

（ii）证明无限单群(这样的群是存在的)没有有限指数 $n>1$ 的子群.

提示：用（i）.

2.98 设 G 是群，$|G|=mp$，其中 p 是素数，$1<m<p$. 证明 G 不是单群.

提示：证明 G 有 p 阶子群 H，并用 G 在 H 的陪集上的表示.

注：现在可以证明小于 60 的数除了 11 个（就是 12，18，24，30，36，40，45，48，50，54，56）之外，都不是非阿贝尔单群的阶. 定理 2.103 排除了所有素数的幂（因为中心恒为正规子群）. 本题排除了所有形为 mp 的数，其中 p 是素数，$m<p$.（用西罗（Sylow）定理可以彻底证明没有阶小于 60 的非阿贝尔单群，见命题 5.41）

2.99 （i）设群 G 作用在集合 X 上，并假设 x，$y\in X$ 位于同一轨道上：有某个 $g\in G$ 使得 $y=gx$. 证明$G_y=gG_xg^{-1}$.

（ii）设有限群 G 作用在集合 X 上. 证明：如果 x，$y\in X$ 位于同一轨道上，则 $|G_x|=|G_y|$.

2.100 旗子由 n 个条幅组成，每个条幅着以 q 种颜色之一，这样的旗子共有多少种？

提示：与 n 的奇偶性有关.

114

2.101 设 X 是 $n\times n$ 网格中的方块，ρ 是 90°旋转. 定义一个（q，G）-着色为一个**棋盘**，其中的作用是 4 阶循环群 $G=\langle\rho\rangle$. 证明棋盘的种数是

$$\frac{1}{4}\left(q^{n^2}+q^{\lfloor(n^2+1)/2\rfloor}+2q^{\lfloor(n^2+3)/4\rfloor}\right),$$

其中$\lfloor x\rfloor$是不超过 x 的最大整数.

2.102 设 X 是等分成 n 个扇形的圆盘，ρ 是旋转（$360/n$）°. 定义一个（q，G）-着色为一个**赌轮**，其中的作用是 n 阶循环群 $G=\langle\rho\rangle$. 证明：如果 $n=6$，则有 6 个扇形的赌轮的种数是 $\frac{1}{6}(2q+2q^2+q^3+q^6)$.

有 n 个扇形的赌轮种数的计算公式是

$$\frac{1}{n}\sum_{d\mid n}\phi(n/d)q^d,$$

其中 ϕ 是欧拉 ϕ-函数.

2.103 设 X 是正 n 边形的顶点，二面体群 $G=D_{2n}$ 作用在它上面(如同通常的对称群，见例 2.28)). 定义正 n 边形的一个 (q, G)-着色为一个**手镯**，称正 n 边形的顶点为**珠子**.(手镯不仅可以转动，还可以抛起来在空中旋转，即沿着连接两粒珠子的直线在空中旋转从而颠倒过来.)

(i) 有 5 粒珠子，每粒着以 q 种颜色之一的手镯有多少种?

提示：作用是群 $G=D_{10}$. 用例 2.28 对每个对称设计顶点的置换，然后证明手镯的数目是

$$\frac{1}{10}(q^5+4q+5q^3).$$

(ii) 有 6 粒珠子，每粒着以 q 种颜色之一的手镯有多少种?

提示：作用是群 $G=D_{12}$. 用例 2.28 对每个对称设计顶点的置换，然后证明手镯的数目是

115

$$\frac{1}{12}(q^6+2q^4+4q^3+3q^2+2q).$$

第3章 交换环 I

3.1 引言

和第1章、第2章一样，本章有些内容通常在早期课程中可以找到，这种结果的证明只有概要，但其他定理有完整的证明. 从引入交换环开始，然后是交换环最突出的例子 $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ 和 $\mathbb{C}$，还有 $\mathbb{I}_m$、多项式、实值函数和有限域. 另外还给出向量空间（标量在任意域上）和线性变换的一些初步结果. 对相似矩阵进行分类的典范型将在第9章中讨论.

3.2 基本性质

从交换环的定义开始.

定义 **交换环**[㊀]是指有加法和乘法两种二元运算的集合 R，满足

（i）R 在加法下是阿贝尔群；

（ii）（**交换性**）对一切 $a,b \in R, ab = ba$；

（iii）（**结合性**）对每个 $a,b,c \in R, a(bc) = (ab)c$；

（iv）存在元素 $1 \in R$，对每个 $a \in R, 1a = a$；[㊁]

（v）（**分配性**）对每个 $a,b,c \in R, a(b+c) = ab + ac$.

116

环 R 中的元素 1 有几个名称，可以叫做一，R 的单位，或 R 的幺元.

交换环中的加法和乘法是二元运算，因此有函数

$$\alpha: R \times R \to R \text{ 为对一切 } r,r' \in R, \alpha(r,r') = r + r' \in R$$

和

$$\mu: R \times R \to R \text{ 为对一切 } r,r' \in R, \mu(r,r') = rr' \in R$$

对于两种运算，代换定律都成立：如果 $r=r'$，$s=s'$，则 $r+s=r'+s'$，$rs=r's'$.

例 3.1 （i）$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ 是具有通常加法和乘法的交换环（环公理在数学基础课程中已得到验证).

（ii）$\mathbb{I}_m$，即整数 mod$m$ 是交换环.

（iii）设 $\mathbb{Z}[i]$ 是所有形为 $a+bi$ 的复数集合，其中 a，$b \in \mathbb{Z}$，$i^2=-1$，$\mathbb{Z}[i]$ 事实上是一个交换环，但验证它是个讨厌的练习（在习题 3.8 中，引入了子环的概念后，证明可大为简化). $\mathbb{Z}[i]$ 叫做**高斯整环**.

（iv）考虑形如

$$x = a + b\omega$$

㊀ 这个术语 ring（环）可能是1897年希尔伯特（Hilbert）在写 Zahlring 时创造的. 德语和英语一样，ring 这个词的一个意思是集团，例如短语"a ring of thieves（一群盗贼）". （也有人提出说希尔伯特用这个词的原因是：对于代数整数环，每个元素的一个适当的幂"转回"到较低幂的线性组合.）

㊁ 有些作者不要求交换环有1，对于他们来说，一切偶整数的集合是交换环，但我们不这样认为.

的全体实数 x 的集合 R，其中 $a,b\in\mathbb{Q},\omega=\sqrt[3]{2}$. 易知 R 在常规加法下封闭. 然而，如果 R 在乘法下封闭，则 $\omega^2\in R$，因而存在有理数 a，b 使得

$$\omega^2=a+b\omega.$$

两端乘以 ω 和 b 得等式

$$2=a\omega+b\omega^2$$
$$b\omega^2=ab+b^2\omega.$$

因此，$2-a\omega=ab+b^2\omega$，于是

$$2-ab=(b^2+a)\omega.$$

如果 $b^2+a\neq 0$，则 $\omega=\sqrt[3]{2}$ 是有理数；如果 $b^2+a=0$，则与 $2-ab=0$ 一起得出 $2=(-b)^3$. 于

117 是不论那种情形都迫使 $\sqrt[3]{2}$ 为有理数，这个矛盾表明 R 不是交换环. ■

注 存在非交换环；即具有加法和乘法两种运算的集合满足交换环的除了公理 $ab=ba$ 外的所有公理. [事实上，该定义把公理 $1a=a$ 换成 $1a=a=a1$，并把分配律换成两个分配律，一个在一边：$a(b+c)=ab+ac$ 和 $(b+c)a=ba+ca$.] 例如，易知一切 $n\times n$ 实数矩阵的集合(配置通常的加法和乘法)满足这种新的环公理. 我们将在第8章中研究非交换环.

下面是一些初步结果.

命题 3.2 设 R 是交换环.

(i) 对每个 $a\in R,0\cdot a=0$.

(ii) 如果 $1=0$，则 R 由单一元素 0 组成. 此时称 R 为**零环**.㊀

(iii) 如果 $-a$ 是 a 的加法逆元，则 $(-1)(-a)=a$.

(iv) 对每个 $a\in R,(-1)a=-a$.

(v) 如果 $n\in\mathbb{N}$ 且 $n1=0$，则对一切 $a\in R,na=0$，其中 $na=a+\cdots+a$ 是 n 个 a 之和.

(vi) 二项式定理成立：如果 a，$b\in R$，则

$$(a+b)^n=\sum_{r=0}^{n}\binom{n}{r}a^rb^{n-r}.$$

证明概要 (i) $0\cdot a=(0+0)\cdot a=0\cdot a+0\cdot a$.

(ii) $a=1\cdot a=0\cdot a=0$.

(iii) $0=(-1+1)(-a)=(-1)(-a)+(-a)$.

(iv) 因 $(-1)(-a)=a$，因而有 $(-1)(-1)(-a)=(-1)a$，但 $(-1)(-1)=1$.

(v) 在第2章中定义了群中元素的幂 a^n，其中 $n\geqslant 0$. 在加法群中，na 是比 a^n 更合适的记号. 对 $n\in\mathbb{N},a\in R$，记号 na 在 R 中也是这种意义，即 na 是 n 个 a 的和.

如果 $a\in R.n\in\mathbb{Z}$ 是正的，则 $n1=0$ 蕴涵

$$na=n(1a)=(n1)a=0a=0.$$

(vi) 对 $n\geqslant 0$ 用归纳法，并用恒等式 $\binom{n+1}{r}=\binom{n}{r-1}+\binom{n}{r}$，其中 $0<r<n+1$.（约定对一切 $a\in R$，甚至 $a=0,a^0=1$.） ■

交换环 R 的子环 S 是包含在比它大的交换环 R 之中的交换环，因此 S 和 R 有相同的加法、乘

㊀ 零环是一个没有多少意思的环，但偶尔会出现.

法和单位.

[118]

定义　称交换环 R 的子集 S 为 R 的**子环**，如果

(i) $1 \in S$;⊖

(ii) 如果 $a,b \in S$，则 $a-b \in S$；

(iii) 如果 $a,b \in S$，则 $ab \in S$.

记号　与子群惯用 $H \leqslant G$ 相比，在环论中习惯用 $S \subseteq R$ 来表示子环，也用 $S \subsetneq R$ 表示真子环；即 $S \subseteq R$ 且 $S \neq R$.

命题 3.3　交换环 R 的子环 S 是交换环.

证明概要　第一个条件是说 S 是加法群 R 的子群，其他条件是恒等式，它们对 R 的一切元素成立，特别对 S 的一切元素也成立. 例如，结合性 $a(bc)=(ab)c$ 对一切 $a,b,c \in R$ 成立，因而特别对一切 a，b，$c \in S \subseteq$ 也成立. ∎

当然，子环概念带来的一个好处是在判定一个交换环的子集自身是否是交换环时，必须验证的环公理可以少一些.

习题 3.4 给出了一个包含在交换环 R 中的交换环 S 的很自然的例子，其中 S 和 R 的加法和乘法相同，但单位不同（由此 S 不是 R 的子环）.

例 3.4　如果 $n \geqslant 3$ 是整数，令 $\zeta = e^{2\pi i/n}$ 为 n 次单位原根. 定义

$$\mathbb{Z}[\zeta_n] = \{z \in \mathbb{C} : z = a_0 + a_1\zeta_n + a_2\zeta_n^2 + \cdots + a_{n-1}\zeta_n^{n-1}, \text{一切 } a_i \in \mathbb{Z}\}.$$

（当 $N=4$ 时，$\mathbb{Z}[\zeta_4]$ 是高斯整环 $\mathbb{Z}[i]$.）容易验证 $\mathbb{Z}[\zeta_n]$ 是 $\mathbb{C}$ 的子环（为了证明 $\mathbb{Z}[\zeta_n]$ 在乘法下封闭，注意如果 $m \geqslant n$，则 $m = qn + r$，其中 $0 \leqslant r < n$，和 $\zeta_n^m = \zeta_n^r$）. ∎

定义　**整环**是指满足两个额外条件的交换环：一是

$$1 \neq 0\text{；}$$

二是乘法的**消去律**成立：对一切 $a,b,c \in R$，

$$\text{如果 } ca = cb \text{ 且 } c \neq 0\text{，则 } a = b.$$

[119]

通常所熟悉的交换环的例子 $\mathbb{Z}$，$\mathbb{Q}$，$\mathbb{R}$ 和 $\mathbb{C}$ 都是整环，零环不是整环.

命题 3.5　非零交换环 R 是整环当且仅当 R 的任两个非零元素的积非零.

证明概要　$ab=ac$ 当且仅当 $a(b-c)=0$. ∎

命题 3.6　交换环 $\mathbb{I}_m$ 是整环当且仅当 m 是素数.

证明　如果 $m=ab$，其中 $1<a,b<m$，则在 $\mathbb{I}_m$ 中 $[a]\neq[0]$，$[b]\neq[0]$，但 $[a][b]=[m]=[0]$.

反之，如果 m 是素数，且 $[a][b]=[ab]=[0]$，则 $m \mid ab$，根据欧几里得引理，$m \mid a$ 或 $m \mid b$. ∎

例 3.7　(i) 设 $\mathcal{F}(\mathbb{R})$ 是一切函数 $\mathbb{R} \to \mathbb{R}$ 的集合，并配置**点态加法**和**点态乘法**：给定 $f,g \in \mathcal{F}(\mathbb{R})$，定义函数 $f+g$ 和 fg 为

$$f+g : a \mapsto f(a)+g(a),\quad fg : a \mapsto f(a)g(a)$$

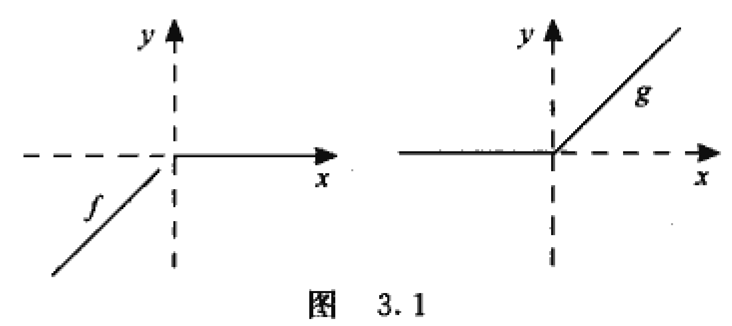
（注意 fg 不是 f 和 g 的复合）.

可断言 $\mathcal{F}(\mathbb{R})$ 连同这些运算是交换环，公理的验证留给读者，这里只给出如下的提示：$\mathcal{F}(\mathbb{R})$ 的零元素是取值 0 的常数函数 z［即对一切 $a \in \mathbb{R}$，$z(a)=0$］，单位是对一切 $a \in \mathbb{R}$，满足 $\varepsilon(a)=1$ 的常数函数 ε. 现在证明 $\mathcal{F}(\mathbb{R})$ 不是整环. 定义 f 和 g 为如图 3.1 所示的函数.

⊖ 偶整数不能形成 $\mathbb{Z}$ 的子环，因为 1 不是偶数. 当引入理想之后，将会认识它们的特殊结构.

$$f(a)=\begin{cases}a & \text{当 } a\leqslant 0\\ 0 & \text{当 } a\geqslant 0\end{cases}\qquad g(a)=\begin{cases}0 & \text{当 } a\leqslant 0\\ a & \text{当 } a\geqslant 0\end{cases}$$

显然 f 和 g 都不为零（即 $f\neq z, g\neq z$）．另一方面，对每个 $a\in\mathbb{R}$，$fg: a\mapsto f(a)g(a)=0$，这是因为因子 $f(a)$ 和 $g(a)$ 中至少一个为数零．所以由命题 1.43 $fg=z$，从而 $\mathcal{F}(\mathbb{R})$ 不是整环．



120

图 3.1

（ⅱ）一切可微函数 $f:\mathbb{R}\to\mathbb{R}$ 形成 $\mathcal{F}(\mathbb{R})$ 的子环，幺元 ε 是常数函数，因而是可微的，而可微函数的和与积也是可微的，所以可微函数形成交换环． ■

许多常规算术定理，即交换环 $\mathbb{Z}$ 的许多性质在更一般的情形也成立，现在把一些熟知的定义从 $\mathbb{Z}$ 推广到任意交换环上．

定义 设 a,b 是交换环 R 的元素，如果存在元素 $c\in R$ 使得 $b=ca$，则称**在 R 中 a 整除 b**（或 a 是 b 的**因子**，或 b 是 a 的**倍数**），记为 $a\mid b$．

作为一个极端的例子，如果 $0\mid a$，则有某个 $b\in R$ 使得 $a=0\cdot b$，然而 $0\cdot b=0$，因此必有 $a=0$．于是 $0\mid a$ 当且仅当 $a=0$．

注意是否有 $a\mid b$ 不仅依赖于元素 a 和 b，而且也依赖于它们所在的环 R．例如，在 $\mathbb{Q}$ 中，3 整除 2，因为 $2=3\times\frac{2}{3}$ 且 $\frac{2}{3}\in\mathbb{Q}$；另一方面，在 $\mathbb{Z}$ 中 3 不整除 2，因为没有整数 c 能使 $3c=2$．

定义 交换环 R 中的元素 u 称为**单位**，如果在 R 中有 $u\mid 1$；即如果存在 $v\in R$ 使得 $uv=1$．称元素 v 为 u 的**逆**，且常记 v 为 u^{-1}．

单位是很重要的，因为任何元素都可被它们整除：如果 $a\in R$ 而 u 是 R 中的单位（由此存在 $v\in R$ 使得 $uv=1$），则对 $va\in R$，

$$a=u(va)$$

是 a 在 R 中的一个因子分解，于是有理由定义商 a/u 为 $va=u^{-1}a$．

给定两个元素 a 和 b，是否 $a\mid b$ 不仅依赖于这两个元素，而且也依赖于所在的环；同样，元素 $u\in R$ 是否是单位也依赖于它所在的环 R（因为这个问题是在 R 中是否有 $u\mid 1$）．例如 2 是 $\mathbb{Q}$ 的单位，因为 $\frac{1}{2}$ 在 $\mathbb{Q}$ 中且 $2\times\frac{1}{2}=1$，但 2 不是 $\mathbb{Z}$ 中的单位，因为没有整数 v 能使得 $2v=1$．事实上，$\mathbb{Z}$ 中的单位只有 1 和 -1．

命题 3.8 设 R 是整环，$a,b\in R$ 非零，则 $a\mid b$ 且 $b\mid a$ 当且仅当有某个单位 $u\in R$ 使得 $b=ua$．

证明概要 如果 $b=ua$ 且 $a=vb$，则 $b=ua=uvb$． ■

存在命题 3.8 不成立的交换环的例子，由此 R 是整环的假设是必须的．

121

$\mathbb{I}_m$ 中的单位是什么？

命题 3.9 如果 a 是整数，则 $[a]$ 是 $\mathbb{I}_m$ 中的单位当且仅当 a 和 m 互素．事实上，如果 $sa+tm=1$，则 $[a]^{-1}=[s]$．

证明概要 $sa\equiv 1\bmod m$ 当且仅当有某个整数 t 使得 $sa+tm=1$． ■

系 3.10 如果 p 是素数，则 $\mathbb{I}_p$ 中的每个非零元素都是单位.

证明概要 如果 $1 \leqslant a < p$，则 $(a,p) = 1$. ■

定义 如果 R 是非零交换环，则称

$$U(R) = \{R \text{ 中的一切单位}\}$$

为 R 的**单位群**.

容易验证 $U(R)$ 是乘法群. 因为群的每个元素有唯一的逆，所以 R 中的单位在 R 中恰有一个逆. 在 $\mathbb{Q}$ 和 $\mathbb{Z}$ 之间存在明显的差别：$\mathbb{Q}$ 的每个非零元素都是单位.

定义 如果 F 是交换环，其中 $1 \neq 0$ 且每个非零元素 a 都是单位；即存在 $a^{-1} \in F$ 使得 $a^{-1}a = 1$，则称 F 为**域**.[㊀]

域的第一批例子是 $\mathbb{Q}$，$\mathbb{R}$ 和 $\mathbb{C}$.

域的定义也可用单位群的术语来表述. 交换环 R 是域当且仅当 $U(R) = R^{\times}$，即 R 的非零元素. 用另一种方式说，R 是域当且仅当 $R^{\times}$ 是乘法群［注意我们假定 $1 \neq 0$，所以 $U(R^{\times}) \neq \varnothing$］.

命题 3.11 每个域 F 都是整环.

证明概要 如果 $ab = ac$ 且 $a \neq 0$，则 $b = a^{-1}(ab) = a^{-1}(ac) = c$. ■

该命题的逆命题不成立，因为 $\mathbb{Z}$ 是整环而不是域.

命题 3.12 交换环 $\mathbb{I}_m$ 是域当且仅当 m 是素数.

证明概要 系 3.10. ■

在定理 3.127 中将看到只要 p 是素数且 $n \geqslant 1$ 就存在恰有 p^n 个元素的有限域；在习题 3.14 中构造了有 4 个元素的域.

整环的每个子环本身也是整环. 因域是整环，所以域的每个子环也是整环. 这个练习的逆命题为真，而且更加重要的是：每个整环都是某个域的子环.

122

给定域 F 的四个元素 a,b,c,d，且 $b \neq 0, d \neq 0$，假定 $ab^{-1} = cd^{-1}$. 两边乘以 bd 得 $ad = bc$. 换句话说，要是把 ab^{-1} 写成 a/b，则刚好证明 $a/b = a/d$ 蕴涵 $ad = bc$，即"交错相乘"是可以使用的. 反之，如果 $ad = bc$，且 b,d 两者都不等于零，则乘以 $b^{-1}d^{-1}$ 得 $ab^{-1} = cd^{-1}$，即 $a/b = c/d$.

通常由整数 $\mathbb{Z}$ 的整环来构造有理数 $\mathbb{Q}$ 的域，下一定理的证明就是这个方法的直接推广.

定理 3.13 如果 R 是整环，则存在包含 R 并把 R 作为子环的域 F. 此外，F 可这样选取：对每个 $f \in F$，存在 $a,b \in R$ 且 $b \neq 0$ 使得 $f = ab^{-1}$.

证明概要 令 $X = \{(a,b) \in R \times R : b \neq 0\}$，定义 X 上的关系 $\equiv$ 为 $(a,b) \equiv (c,d)$ 如果 $ad = bc$. 可断言 $\equiv$ 是等价关系. 容易验证自反性和对称性，这里给出传递性的证明. 如果 $(a,b) \equiv (c,d)$，$(c,d) \equiv (e,f)$，则 $ad = bc, cf = de$. 但由 $ad = bc$ 得 $adf = b(cf) = bde$，因 d 非零，消去 d 得 $af = be$，即 $(a,b) \equiv (e,f)$.

记 (a,b) 的等价类为 $[a,b]$，定义 F 为一切等价类 $[a,b]$ 的集合，配置 F 以下面的加法和乘法(如果我们妄自把 $[a,b]$ 当作分数 a/b，那么下面就是通常的公式)：

$$[a,b] + [c,d] = [ad + bc, bd]$$

㊀ 英语术语 field（域）的数学用法的引入（1893 年穆尔（E. H. Moore）在他的有限域分类的论文中第一次使用）如同德语术语 körper 和法语术语 corps 一样，类似于 group（群）和 ring（环）的引入，这些单词都表示"范围"或"事物的集团". 单词 domain（整环）是德语 integretätsbereich 的通常英语翻译 integral domain 的简化，意思是整数的集团.

和

$$[a,b][c,d] = [ac,bd].$$

首先，因 $b \neq 0, d \neq 0$，所以有 $bd \neq 0$，这是因为 R 是整环，从而上面的公式是有意义的. 现在证明加法是合理定义的. 如果 $[a,b] = [a',b']$（即 $ab' = a'b$），$[c,d] = [c',d']$（即 $cd' = c'd$），则必须证明 $[ad+bc,bd] = [a'd'+b'c',b'd']$，但该式是成立的：

$$(ad+bc)b'd' = ab'dd' + bb'cd' = a'bdd' + bb'c'd = (a'd'+b'c')bd.$$

类似的讨论可证明乘法是合理定义的.

现在容易验证 F 是交换环：零元素是 $[0,1]$，幺元是 $[1,1]$，$[a,b]$ 的加法逆是 $[-a,-b]$. 易知族 $R' = \{[a,1] : a \in R\}$ 是 F 的子环，我们把 $a \in R$ 等同于 $[a,1] \in R'$.

为了证明 F 是域，注意到如果 $[a,b] \neq [0,1]$，则 $a \neq 0$，从而 $[a,b]$ 的逆是 $[b,a]$.

最后，如果 $b \neq 0$，则 $[1,b] = [b,1]^{-1}$，从而 $[a,b] = [a,1][b,1]^{-1}$. ■

定义 定理 3.13 中由 R 构成的域 F 称为 R 的**分式域**，记为 $\mathrm{Frac}(R)$，且记 $[a,b] \in \mathrm{Frac}(R)$ 为 a/b. 特别地，R' 的元素 $[a,1]$ 记为 $a/1$ 或更简单地记为 a.

123

注意$\mathbb{Z}$ 的分式域是$\mathbb{Q}$，即 $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$.

定义 域 K 的**子域**是 K 的子环 k，它也是一个域.

易知域 K 的子集 k 是子域当且仅当 k 是在逆之下封闭的子环；即，如果 $a \in k$ 且 $a \neq 0$，则 $a^{-1} \in k$. 显然，K 的子域的交自身也是 K 的子域（注意交不等于 $\{0\}$，因为 1 在每个子域中）.

习题

3.1 证明交换环 R 中 1 是唯一的.

3.2 （i）证明$\mathbb{Z}$ 中的减法不是结合运算.

（ii）举出一个交换环 R 的例子，其中减法是结合的.

3.3 （i）如果 R 是整环，$a \in R$ 满足 $a^2 = a$，证明不是 $a = 0$ 就是 $a = 1$.

（ii）证明例 2.7 中的交换环 $\mathcal{F}(\mathbb{R})$ 包含无限多个元素 f 满足 $f \neq 0,1$ 且 $f^2 = f$.

3.4 （i）如果 X 是集合，$\mathcal{B}(X)$ 是例 2.18 定义的布尔（Boole）群，它的元素是 X 的子集，它的加法由

$$U + V = (U - V) \cup (V - U)$$

给出，其中 $U - V = \{x \in U : x \notin V\}$. 如果再定义乘法如下：

$$UV = U \cap V.$$

证明 $\mathcal{B}(X)$ 是交换环. 我们称 $\mathcal{B}(X)$ 为**布尔环**.

提示：可用集合论的一些通常事实：分配律：$U \cap (V \cup W) = (U \cap V) \cup (U \cap W)$. 如果 V' 表示 V 的补集，则 $U - V = U \cap V'$. **德摩根**（De Morgan）**定律**：$(U \cap V)' = U' \cup V'$.

（ii）证明 $\mathcal{B}(X)$ 恰包含一个单位.

（iii）如果 Y 是 X 的真子集（即 $Y \subsetneq X$），则 $\mathcal{B}(Y)$ 中的单位与 $\mathcal{B}(X)$ 中的单位不同. 由此可知 $\mathcal{B}(Y)$ 不是 $\mathcal{B}(X)$ 的子环.

3.5 证明 $U(\mathbb{I}_m) = \{[k] \in \mathbb{I}_m : (k,m) = 1\}$.

3.6 求例 3.7 中定义的交换环 $\mathcal{F}(\mathbb{R})$ 中的所有单位.

3.7 把 $\mathcal{F}(\mathbb{R})$ 的构造法推广到任意交换环 R 上：设 $\mathcal{F}(R)$ 是 R 到 R 的所有函数的集合，并配置点态加法，对 $r \in R$：$f + g : r \mapsto f(r) + g(r)$；点态乘法：$fg : r \mapsto f(r)g(r)$.

（i）证明 $\mathcal{F}(R)$ 是交换环.

（ii）证明 $\mathcal{F}(R)$ 不是整环.

（iii）证明 $\mathcal{F}(\mathbb{I}_2)$ 恰有四个元素，且对每个 $f \in \mathcal{F}(\mathbb{I}_2), f+f=0$.

3.8 （i）如果 R 是整环且 S 是 R 的子环，则 S 是整环.

（ii）证明$\mathbb{C}$是整环，并推导出高斯整数环是整环.

3.9 证明$\mathbb{Z}$的唯一子环是$\mathbb{Z}$自己.

提示：$\mathbb{Z}$ 的每个子环 R 包含 1.

124

3.10 （i）证明 $R=\{a+b\sqrt{2}: a,b \in \mathbb{Z}\}$ 是整环.

（ii）证明 $R=\{\frac{1}{2}(a+b\sqrt{2}): a,b \in \mathbb{Z}\}$ 不是整环.

（iii）用 $\alpha=\frac{1}{2}(1+\sqrt{-19})$ 是 x^2-x+5 的根的事实，证明 $R=\{a+b\alpha: a,b \in \mathbb{Z}\}$ 是整环.

3.11 证明一切 C^∞- 函数的集合是 $\mathcal{F}(\mathbb{R})$ 的子环.（如果函数 $f:\mathbb{R}\to\mathbb{R}$ 对每个 $n\geq 1$ 具有 n 阶导数 $f^{(n)}$，则 $f:\mathbb{R}\to\mathbb{R}$ 是一个 C^∞- 函数）

提示：用莱布尼茨法则（见习题 1.6）.

3.12 （i）如果 R 是交换环，定义**圈运算** $a\circ b$ 为

$$a\circ b=a+b-ab.$$

证明圈运算是结合的且对一切 $a\in R, 0\circ a=a$.

（ii）证明交换环 R 是域当且仅当 $\{r\in R: r\neq 1\}$ 在圈运算下是阿贝尔群.

提示：如果 $a\neq 0$，则 $a+1\neq 1$.

3.13 求 $\mathbb{I}_{11}$ 的非零元素的逆.

3.14 (R. A. Dean) 定义 $\mathbb{F}_4$ 为形如

$$\begin{bmatrix} a & b \\ b & a+b \end{bmatrix}$$

的一切 2×2 矩阵，其中 $a,b\in\mathbb{I}_2$.

（i）证明 $\mathbb{F}_4$ 在通常矩阵加法和乘法运算下是交换环.

（ii）证明 $\mathbb{F}_4$ 是恰有四个元素的域.

3.15 证明元素有限的整环 R 必是域.（利用命题 3.6，本题给出命题 3.12 中充分性的一个新证明.）

提示：用 $R^\times$ 记 R 中的非零元素的集合，证明乘 r 是单射 $R^\times\to R^\times$，其中 $r\in R^\times$.

3.16 证明 $F=\{a+b\sqrt{2}: a,b\in\mathbb{Q}\}$ 是域.

3.17 （i）证明 $F=\{a+bi: a,b\in\mathbb{Q}\}$ 是域.

（ii）证明 F 是高斯整数的分式域.

3.18 如果 R 是交换环，定义 R 上的关系$\equiv$为 $a\equiv b$，如果存在单位 $u\in R$ 使得 $b=ua$. 证明：如果 $a\equiv b$，则 $(a)=(b)$，其中 $(a)=\{ra: r\in R\}$. 反之，证明：如果 R 是整环，则 $(a)=(b)$ 蕴涵 $a\equiv b$.

3.19 （i）对任意域 k，证明**随机群** $\Sigma(2,k)$ 在矩阵乘法下是群，其中随机群 $\Sigma(2,k)$ 是元素在 k 中，每列的和为 1 的一切 2×2 非奇异矩阵.

（ii）定义**放射群** $\mathrm{Aff}(1,k)$ 为形如 $f(x)=ax+b$ 的一切 $f:k\to k$ 的集合，其中 $a,b\in k, a\neq 0$. 证明 $\Sigma(2,k)\cong\mathrm{Aff}(1,k)$.（见习题 2.46.）

（iii）如果 k 是有 q 个元素的有限域，证明 $|\Sigma(2,k)|=q(q-1)$.

（iv）证明 $\Sigma(2,\mathbb{I}_3)\cong S_3$.

125

3.3 多项式

虽然读者对多项式是熟悉的，我们还是要小心地引入多项式，所要注意的关键是多项式的系数

在什么范围内.

定义 如果 R 是交换环，则 R 中的**序列**σ 是指

$$\sigma=(s_0,s_1,s_2,\cdots,s_i,\cdots);$$

其中对一切 $i\geqslant 0, s_i\in R$，并称之为 σ 的**系数**.

为了确定两个序列什么时候相等，我们认清序列 σ 其实就是一个函数 $\sigma:\mathbf{N}\to R$，其中N是自然数的集合，且对一切 $i\geqslant 0,\sigma(i)=s_i$. 于是，如果 $\tau=(t_0,t_1,t_2,\cdots,t_i,\cdots)$ 也是一个序列，则 $\sigma=\tau$ 当且仅当对一切 $i\geqslant 0,\sigma(i)=\tau(i)$，即 $\sigma=\tau$ 当且仅当对一切 $i\geqslant 0,s_i=t_i$.

定义 交换环 R 中的序列 $\sigma=(s_0,s_1,s_2,\cdots,s_i,\cdots)$ 称为**多项式**，如果存在整数 $m\geqslant 0$ 使得对一切 $i>m,s_i=0$；即

$$\sigma=(s_0,s_1,\cdots,s_m,0,0,\cdots).$$

多项式只有有限个非零系数. **零多项式**是序列 $\sigma=(0,0,0\cdots)$，记为 $\sigma=0$.

定义 如果 $\sigma=(s_0,s_1,s_2,\cdots,s_n,0,0,\cdots)\neq 0$ 是多项式，则存在 $s_n\neq 0$ 使得对一切 $i>n,s_i=0$. 称 s_n 为 σ 的**首项系数**，称 n 为 σ 的**次数**，并记次数 n 为 $\deg(\sigma)$.

零多项式 0 没有次数，因为它没有非零系数. 有些作者定义 $\deg(0)=-\infty$，有时候这是方便的，因为对每个整数 $n,-\infty<n$. 另一方面，因为它经常是一种真正不同的情形，必须分别对待，所以我们选择零多项式没有次数.

记号 如果 R 是交换环，则系数在 R 中的一切多项式的集合记为 $R[x]$.

命题 3.14 如果 R 是交换环，则 $R[x]$ 也是交换环，它包含 R 作为它的子环.

证明概要 定义多项式的加法和乘法如下：如果 $\sigma=(s_0,s_1,\cdots),\tau=(t_0,t_1\cdots)$，则

$$\sigma+\tau=(s_0+t_0,s_1+t_1,\cdots,s_n+t_n,\cdots)$$

和

126

$$\sigma\tau=(c_0,c_1,c_2,\cdots),$$

其中 $c_k=\sum_{i+j=k}s_it_j=\sum_{i=0}^{k}s_it_{k-i}$. 验证定义交换环的公理是简单的. 子集 $\{(r,0,0,\cdots):r\in R\}$ 是 $R[x]$ 的子环，我们把它等同于 R. ■

引理 3.15 设 R 是交换环并设 $\sigma,\tau\in R[x]$ 是非零多项式.

(i) 或者 $\sigma\tau=0$，或者 $\deg(\sigma\tau)\leqslant\deg(\sigma)+\deg(\tau)$.

(ii) 如果 R 是整环，则 $\sigma\tau\neq 0$ 且

$$\deg(\sigma\tau)=\deg(\sigma)+\deg(\tau).$$

(iii) 如果 R 是整环，则 $R[x]$ 也是整环.

证明概要 设 $\sigma=(s_0,s_1,\cdots),\tau=(t_0,t_1\cdots)$ 分别有次数 m 和 n.

(i) 如果 $k>m+n$，则 $\sum_i s_it_{k-i}$ 中每一项都是 0（因为不是 $s_i=0$，就是 $t_{k-i}=0$).

(ii) $\sum_i s_it_{m+n-i}$ 中每一项都是 0，除了可能的例外 s_mt_n. 因为 R 是整环，所以 $s_m\neq 0,t_n\neq 0$ 蕴涵 $s_mt_n\neq 0$.

(iii) 由 (ii)，两个非零多项式的积非零，因此结论成立. ■

定义 如果 R 是交换环，则称 $R[x]$ 为 R **上的多项式环**.

下面是以上的讨论和通常记号之间的联系.

定义 定义元素 $x\in R[x]$ 为

$$x = (0,1,0,0,\cdots).$$

引理 3.16 （i）如果 $\sigma = (s_0, s_1, \cdots)$，则

$$x\sigma = (0, s_0, s_1, \cdots);$$

即，乘 x 就是把每个系数向右推移一步.

（ii）如果 $n \geq 1$，则 x^n 是第 n 个坐标为 1，其他全为 0 的多项式.

（iii）如果 $r \in R$，则

$$(r,0,0,\cdots)(s_0, s_1, \cdots s_j, \cdots) = (rs_0, rs_1, \cdots, rs_j, \cdots).$$

证明概要 用多项式乘法定义再经简单计算便可得结论. ■ [127]

如果把 $(r,0,0,\cdots)$ 等同于 r，则引理 3.16（iii）可理解为

$$r(s_0, s_1, \cdots, s_i, \cdots) = (rs_0, rs_1, \cdots, rs_i, \cdots).$$

我们现在可以重新恢复到通常的记号.

命题 3.17 如果 $\sigma = (s_0, s_1, \cdots, s_n, 0, 0, \cdots)$，则

$$\sigma = s_0 + s_1 x + s_2 x^2 + \cdots + s_n x^n,$$

其中每个元素 $s \in R$ 等同于多项式 $(s,0,0,\cdots)$.

证明

$$\begin{aligned}\sigma &= (s_0, s_1, \cdots, s_n, 0, 0, \cdots)\\ &= (s_0, 0, 0, \cdots) + (0, s_1, 0, \cdots) + \cdots + (0, 0, \cdots, s_n, 0, \cdots)\\ &= s_0(1,0,0,\cdots) + s_1(0,1,0,\cdots) + \cdots + s_n(0,0,\cdots,1,0,\cdots)\\ &= s_0 + s_1 x + s_2 x^2 + \cdots + s_n x^n.\end{aligned}$$

■

从现在起我们使用这个熟悉的（通常的）记号. 和习惯的一样，我们用

$$f(x) = s_0 + s_1 x + s_2 x^2 + \cdots + s_n x^n$$

代替 $\sigma = (s_0, s_1, \cdots, s_n, 0, 0, \cdots)$.

下面是有关多项式的一些通常的名称. 如果 $f(x) = s_0 + s_1 x + s_2 x^2 + \cdots + s_n x^n$，其中 $s_n \neq 0$，则称 s_0 为**常数项**，称 s_n 为**首项系数**，如我们已经称呼的那样. 如果首项系数 $s_n = 1$，则称 $f(x)$ 为**首一多项式**. 除零多项式 0（所有系数都为 0）之外每个多项式都有次数. **常数多项式**不是零多项式就是次数为 0 的多项式. 次数为 1 的多项式，即 $a + bx$，其中 $b \neq 0$，称为**线性**多项式. 次数为 2 的多项式称为**二次**[⊖]多项式，次数为 3 的称为**三次**多项式，然后是**四次**、**五次**等等.

系 3.18 次数分别为 n 和 m 的多项式 $f(x) = s_0 + s_1 x + s_2 x^2 + \cdots + s_n x^n$ 和 $g(x) = t_0 + t_1 x + t_2 x^2 + \cdots + t_m x^m$ 相等当且仅当 $n = m$ 且对一切 $i, s_i = t_i$.

证明 这只是序列相等定义的复述，再换成多项式的通常记号. ■ [128]

我们现在可以描述 $f(x)$ 中通常作为变量出现的 x. 如果 R 是交换环，则每个多项式 $f(x) = s_0 + s_1 x + s_2 x^2 + \cdots + s_n x^n \in R[x]$ 由赋值定义了一个**多项式函数** $f: R \to R$，即如果 $a \in R$，则定义 $f(a) = s_0 + s_1 a + s_2 a^2 + \cdots + s_n a^n \in R$. 读者应明白多项式和多项式函数是不同的对象. 例如，假定 R 是有限环（比如 $R = \mathbb{I}_m$），则只有有限个函数从 R 到它自身，从而只有有限个多项式函数. 另一方面，多项式有无限个：例如根据系 3.18，一切幂 $1, x, x^2, \cdots, x^n, \cdots$

⊖ 之所以称为 quadratic（二次）多项式是因为一个特别的二次多项式 x^2 给出了正方形的面积（quadratic 来自意为"四"的拉丁字，提醒我们这是一个四边形）. 类似地，之所以称为 cubic（三次）多项式是因为 x^3 给出了立方体的体积. 称线性多项式是因为 $\mathbb{R}[x]$ 中线性多项式的图像是一条直线.

都是不同的.

定义 设 k 是域. $k[x]$ 的分式域记为 $k(x)$，称为 k 上的**有理函数域**.

命题 3.19 如果 k 是域，则 $k(x)$ 的元素形如 $f(x)/g(x)$，其中 $f(x),g(x)\in k[x]$，且 $g(x)\neq 0$.

证明概要 定理 3.13. ■

命题 3.20 如果 p 是素数，则有理函数域 $\mathbb{I}_p(x)$ 是包含 $\mathbb{I}_p$ 作为子域㊀的无限域.

证明 由引理 3.15（ⅲ），$\mathbb{I}_p[x]$ 是无限整环，因为对于 $n\in\mathbb{N}$，幂 x^n 都不同. 于是它的分式域 $\mathbb{I}_p(x)$ 是包含 $\mathbb{I}_p[x]$ 作为子环的无限域. 而由命题 3.14，$\mathbb{I}_p[x]$ 包含 $\mathbb{I}_p$ 作为子环. ■

尽管多项式和多项式函数之间有差别（在系 3.28 中，我们将看到当系数环 R 是无限域时，两个对象是一致的），$R[x]$ 常称为 R 上的一元多项式环. 如果记 $A=R[x]$，则称多项式环 $A[y]$ 为 R 上的两个变量 x,y 的多项式环，并记为 $R[x,y]$. 例如，二次多项式 $ax^2+bxy+cy^2+dx+ey+f$ 可以写成 $cy^2+(bx+e)y+(ax^2+dx+f)$，它是一个系数在 $R[x]$中的 y 的多项式. 用归纳法可构成系数在 R 中的一切 n 个变量的多项式的交换环 $R[x_1,x_2,\cdots,x_n]$. 现在引理3.15（ⅲ）可以对 n 用归纳法推广为如果 R 是整环，则 $R[x_1,x_2,\cdots x_n]$ 也是整环. 此外，当 k 是域时，可以把 $\mathrm{Frac}(k[x_1,x_2,\cdots,x_n])$ 描述为一切 n 个变量的**有理函数**，它的元素形如 $f(x_1,x_2,\cdots,x_n)/g(x_1,x_2,\cdots,x_n)$，其中 f,g 在 $k[x_1,x_2,\cdots,x_n]$ 中.

习题

3.20 证明：如果 R 是交换环，则 $R[x]$ 永不为域.

129

提示：如果 x^{-1} 存在，它的次数是什么？

3.21 （ⅰ）设 R 是整环，证明：如果 $R[x]$中的一个多项式是单位，则它必是非零常数（如果 R 是域，则逆命题也成立）.

提示：计算次数.

（ⅱ）证明在 $\mathbb{I}_4[x]$ 中$(2x+1)^2=1$. 由此可知，（ⅰ）中有必要假设 R 是整环.

3.22 证明定义为 $f(x)=x^p-x\in\mathbb{I}_p[x]$ 的多项式函数恒等于零.

3.23 如果 R 是交换环且 $f(x)=\sum_{i=0}^{n}s_ix^i\in R[x]$的次数 $n\geqslant 1$，定义它的**导数**$f'(x)\in R[x]$ 为

$$f'(x)=s_1+2s_2x+3s_3x^2+\cdots+ns_nx^{n-1};$$

如果 $f(x)$是常数多项式，则定义它的导数为零多项式. 证明微积分的通常法则成立：

$$(f+g)'=f'+g';$$

$$\text{如果 } r\in R\text{，则 } (rf)'=r(f');$$

$$(fg)'=fg'+f'g;$$

$$\text{对一切 } n\geqslant 1,(f^n)'=nf^{n-1}f'.$$

3.24 设 R 是交换环，并设 $f(x)\in R[x]$.

（ⅰ）证明：在 $R[x]$ 中，如果 $(x-a)^2\mid f(x)$，则 $x-a\mid f'(x)$.

（ⅱ）证明：如果 $x-a\mid f(x)$ 且 $x-a\mid f'(x)$，则 $(x-a)^2\mid f(x)$.

3.25 （ⅰ）如果 $f(x)=ax^{2p}+bx^p+c\in\mathbb{I}_p[x]$，证明 $f'(x)=0$.

（ⅱ）证明多项式 $f(x)\in\mathbb{I}_p[x]$ 满足 $f'(x)=0$ 当且仅当存在多项式 $g(x)=\sum a_nx^n$ 使得 $f(x)=g(x^p)$；即 $f(x)=\sum a_nx^{np}\in\mathbb{I}_p[x^p]$.

㊀ 以后，当把$\mathbb{I}_p$ 看作域时记为$\mathbb{F}_p$.

3.26 如果 R 是交换环，定义 $R[[x]]$ 为一切序列 $(s_0, s_1 \cdots)$ 的集合，其中对一切 $i, s_i \in R$（这里不假定对大的 i 有 $s_i = 0$）.

(i) 证明 $R[x]$ 上定义加法和乘法的公式对 $R[[x]]$ 也有意义，并在这些运算下 $R[[x]]$ 是交换环.（称 $R[[x]]$ 为 R 上的**形式幂级数环**.）

(ii) 证明 $R[x]$ 是 $R[[x]]$ 的子环.

(iii) 证明：如果 R 是整环，则 $R[[x]]$ 也是整环.

提示：如果 $\sigma = (s_0, s_1, \cdots) \in R[[x]]$ 非零，定义 σ 的阶为满足 $s_n \neq 0$ 的最小 $n \geq 0$，记为 $\mathrm{ord}(\sigma)$. 如果 R 是整环，$\sigma, \tau \in R[[x]]$ 非零，证明 $\mathrm{ord}(\sigma\tau) = \mathrm{ord}(\sigma) + \mathrm{ord}(\tau) \neq 0$，因此 $\sigma\tau \neq 0$.

3.27 (i) 记形式幂级数 $\sigma = (s_0, s_1, s_2, \cdots, s_n, \cdots)$ 为

$$\sigma = s_0 + s_1 x + s_2 x^2 + \cdots.$$

证明：如果 $\sigma = 1 + x + x^2 + \cdots$，则在 $R[[x]]$ 中 $\sigma = 1/(1-x)$，即 $(1-x)\sigma = 1$.

(ii) 证明：如果 k 是域，则形式幂级数 $\sigma \in k[[x]]$ 是单位当且仅当它的常数项非零；即 $\mathrm{ord}(\sigma) = 0$.

(iii) 设 $\sigma \in k[[x]]$ 且 $\mathrm{ord}(\sigma) = n$，证明

$$\sigma = x^n u,$$

其中 u 是 $k[[x]]$ 中的单位.

130

3.4 最大公因式

我们将看到当 k 是域时，事实上所有对 $\mathbb{Z}$ 证明的熟知的定理对 $k[x]$ 中的多项式也有类似的定理，并且，我们所熟知的证明也可以翻译过来变成这里的证明.

系数在域中的多项式的带余除法说明长除法是可行的.

定理 3.21（带余除法） *假定 k 是域，$f(x), g(x) \in k[x]$ 且 $f(x) \neq 0$，则存在唯一的多项式 $q(x), r(x) \in k[x]$ 使得*

$$g(x) = q(x)f(x) + r(x),$$

并且或者 $r(x) = 0$ 或者 $\deg(r) < \deg(f)$.

证明 先证明 q 和 r 的存在性. 如果 $f \mid g$，则对某个 q 有 $g = qf$. 定义余式 $r = 0$ 就可以了. 如果 $f \nmid g$，则考虑一切形如 $g - qf$（必定非零）的多项式，其中 q 遍历 $k[x]$. 最小整数公理保证在所有这些多项式中有一个次数最小的 $r = g - qf$. 因 $g = qf + r$，所以只需证明 $\deg(r) < \deg(f)$. 记 $f(x) = s_n x^n + \cdots + s_1 x + s_0$，$r(x) = t_m x^m + \cdots + t_1 x + t_0$. 现在 $s_n \neq 0$ 蕴涵 s_n 是一个单位，这是因为 k 是域，因而 k 中存在 s_n^{-1}. 如果 $\deg(r) \geq \deg(f)$，定义

$$h(x) = r(x) - t_m s_n^{-1} x^{m-n} f(x);$$

即如果 $\mathrm{LT}(f) = s_n x^n$，其中 LT 代表首项，则

$$h = r - \frac{\mathrm{LT}(r)}{\mathrm{LT}(f)} f;$$

注意或者 $h = 0$，或者 $\deg(h) < \deg(r)$. 如果 $h = 0$，则 $r = [\mathrm{LT}(r)/\mathrm{LT}(f)]f$ 且

$$\begin{aligned} g &= qf + r \\ &= qf + \frac{\mathrm{LT}(r)}{\mathrm{LT}(f)} f \\ &= \left[q + \frac{\mathrm{LT}(r)}{\mathrm{LT}(f)}\right] f, \end{aligned}$$

与 $f \nmid g$ 矛盾. 如果 $h \neq 0$，则 $\deg(h) < \deg(r)$ 且

$$g-qf=r=h+\frac{\mathrm{LT}(r)}{\mathrm{LT}(f)}f.$$

于是 $g-[q+\mathrm{LT}(r)/\mathrm{LT}(f)]f=h$，与 r 是具有这种形式的次数最小的多项式矛盾．所以 $\deg(r)<\deg(f)$．

131

为了证明 $q(x)$ 和 $r(x)$ 的唯一性，假定 $g=q'f+r'$，其中 $\deg(r')<\deg(f)$．则

$$(q-q')f=r'-r.$$

如果 $r'\neq r$，则两端都有次数．但 $\deg((q-q')f)=\deg(q-q')+\deg(f)\geqslant\deg(f)$，而 $\deg(r'-r)\leqslant\max\{\deg(r'),\deg(r)\}<\deg(f)$，这便产生矛盾．因此 $r'=r$，且 $(q-q')f=0$．因为 $k[x]$ 是域且 $f\neq 0$，从而 $q-q'=0,q=q'$． ■

定义 如果 $f(x)$ 和 $g(x)$ 是 $k[x]$ 中的多项式，其中 k 是域，则带余除法中出现的多项式 $q(x)$ 和 $r(x)$ 称为 $g(x)$ 除以 $f(x)$ 的**商**和**余式**．

k 是域的假设太强，对每个交换环 R，长除法在 $R[x]$ 中都可以进行，只要 $f(x)$ 的首项系数是 R 的单位．特别地，当 $f(x)$ 是首一多项式时，长除法总是可以进行的．

系 3.22 设 R 是交换环，$f(x)\in R[x]$ 是首一多项式．如果 $g(x)\in R[x]$，则存在 $q(x),r(x)\in R[x]$ 使得

$$g(x)=q(x)f(x)+r(x),$$

其中或者 $r(x)=0$或者 $\deg(r)<\deg(f)$．

证明概要 这里可以重复带余除法的证明，只要注意到 $\mathrm{LT}(r)/\mathrm{LT}(f)\in R$，这是因为 $f(x)$ 是首一多项式． ■

现在我们把注意力转移到多项式的根．

定义 如果 $f(x)\in k[x]$，其中 k 是域，则 $f(x)$ **在 k 中的根**是满足 $f(a)=0$ 的元素 $a\in k$．

注 多项式 $f(x)=x^2-2$ 的系数在$\mathbb{Q}$中，但我们常说$\sqrt{2}$是 $f(x)$ 的一个根，即使$\sqrt{2}$是无理数，即 $\sqrt{2}\notin\mathbb{Q}$．在后面的定理 3.123 中我们将看到对每个多项式 $f(x)\in k[x]$，其中 k 是任意域，存在包含 k 并把它作为子域的更大的域 E，它包含 $f(x)$ 所有的根．例如 $x^2-2\in\mathbb{I}_3[x]$ 在$\mathbb{I}_3$ 中没有根，但我们将看到在包含 $\mathbb{I}_3$ 的某个（有限）域中存在类似$\sqrt{2}$的元素．

在下一个引理的证明中，我们要用到下面的初等练习．设 $f(x),g(x)\in R[x]$，其中 R 是交换环，记

$$a(x)=f(x)+g(x) \text{ 和 } m(x)=f(x)g(x)\text{；}$$

132

计算在 $u\in R$ 处的值得 $a(u)=f(u)+g(u),m(u)=f(u)g(u)$．

引理 3.23 设 $f(x)\in k[x]$，其中 k 是域，并设 $u\in k$，则存在 $q(x)\in k[x]$ 使得

$$f(x)=q(x)(x-u)+f(u).$$

证明 带余除法给出

$$f(x)=q(x)(x-u)+r;$$

余式 r 是常数，因为 $x-u$ 的次数为 1．现在计算值

$$f(u)=q(u)(u-u)+r,$$

从而 $r=f(u)$． ■

根和因式分解间存在一种联系．

命题 3.24 如果 $f(x)\in k[x]$，其中 k 是域，则 a 是 $f(x)$ 在 k 中的根当且仅当在 $k[x]$ 中 $x-a$ 整

除 $f(x)$.

证明 如果 a 是 $f(x)$ 在 k 中的根，则 $f(a)=0$，且引理给出 $f(x)=q(x)(x-a)$. 反之，如果 $f(x)=g(x)(x-a)$，则计算它在 a 处的值得 $f(a)=g(a)(a-a)=0$. ■

定理 3.25 设 k 是域，$f(x)\in k[x]$. 如果 $f(x)$ 的次数为 n，则 $f(x)$ 在 k 中至多有 n 个根.

证明 对 $n\geqslant 0$ 用归纳法证明该陈述. 如果 $n=0$，则 $f(x)$ 是非零常数，因此它在 k 中根的个数为零. 现在设 $n>0$. 如果 $f(x)$ 在 k 中没有根，则因 $0\leqslant n$，结论已经成立. 否则，可以假定 $a\in k$ 是 $f(x)$ 的一个根，由命题 3.24，

$$f(x)=q(x)(x-a);$$

此外，$q(x)\in k[x]$ 的次数为 $n-1$. 如果还有根 $b\in k$ 且 $b\neq a$，则

$$0=f(b)=q(b)(b-a).$$

因为 $b-a\neq 0$，所以有 $q(b)=0$（因为 k 是域，因而是整环），从而 b 是 $q(x)$ 的根. 现在 $\deg(q)=n-1$，从而归纳假设说 $q(x)$ 在 k 中至多有 $n-1$ 个根. 所以 $f(x)$ 在 k 中至多有 n 个根. ■

例 3.26 如果多项式的系数在任意交换环 R 中，则定理 3.25 不成立. 例如，如果 $R=\mathbb{I}_8$，则二次多项式 $x^2-1\in\mathbb{I}_8[x]$ 有 4 个根：$[1],[3],[5]$ 和 $[7]$. ■

133

系 3.27 $\mathbb{C}$ 中每个 n 次单位根等于

$$e^{2\pi ik/n}=\cos\left(\frac{2\pi k}{n}\right)+i\sin\left(\frac{2\pi k}{n}\right),$$

其中 $k=0,1,2,\cdots,n-1$.

证明 在系 1.35 中已知这 n 个不同的复数 $e^{2\pi ik/n}$ 是 n 次单位根；即它们都是 x^n-1 的根. 由定理 3.25，不可能有其他的复根. ■

回顾每个多项式 $f(x)\in k[x]$ 都确定了多项式函数 $k\to k$，对一切 $a\in k$，该函数把 a 发送到 $f(a)$. 然而，在习题 3.22 中我们看到 $\mathbb{I}_p[x]$ 中的一个非零多项式（例如 x^p-x）能够确定常数函数零. 当域 k 为无限时，该反常状态消失.

系 3.28 设 k 是无限域，$f(x)$ 和 $g(x)$ 是 $k[x]$ 中的多项式. 如果 $f(x)$ 和 $g(x)$ 确定同一个多项式函数 [即如果对一切 $a\in k,f(a)=g(a)$]，则 $f(x)=g(x)$.

证明 如果 $f(x)\neq g(x)$，则多项式 $h(x)=f(x)-g(x)$ 非零，因此它有某个次数，比如 n 次. 现在 k 中每个元素都是 $h(x)$ 的根，因 k 无限，所以 $h(x)$ 的根多于 n 个，这与定理矛盾. ■

这个证明产生了一个更一般的结果.

系 3.29 设 k 是任意域，可以是有限域. 如果 $f(x),g(x)\in k[x],\deg(f)\leqslant\deg(g)\leqslant n$，且对于 $n+1$ 个元素 $a\in k$ 有 $f(a)=g(a)$，则 $f(x)=g(x)$.

证明概要 如果 $f\neq g$，则 $\deg(f-g)$ 有定义且 $\deg(f-g)\leqslant n$. ■

下面是定理 3.25 的另一个很好的应用.

定理 3.30 如果 k 是域，G 是乘法群 $k^\times$ 的有限子群，则 G 是循环群. 特别地，如果 k 本身有限(比如 $k=\mathbb{I}_p$)，则 $k^\times$ 是循环群.

证明 设 d 是 $|G|$ 的因数. 如果 G 有两个 d 阶子群，比如 S 和 T，则 $|S\cup T|>d$. 而由拉格朗日定理，每个 $a\in S\cup T$ 满足 $a^d=1$，从而是 x^d-1 的根. 现在这个多项式在 k 中有太多的根，与定理 3.25 矛盾. 因此由定理 2.86，G 是循环群. ■

定义 如果 k 是有限域，则循环群 $k^\times$ 的生成元称为 k 的**本原元**.

虽然乘法群 $\mathbb{I}_p^\times$ 是循环群，却没有已知的明确公式可以给出它的每一个本原元. 例如，求 $\mathbb{F}_{257}$ 的本原元，本质上是要验证每个 $[i]$ 的幂，其中 $1 < i < 257$，直到发现对所有的正整数 $m < 256$，$i^m \not\equiv 1 \bmod 257$.

134

多项式的最大公因式的定义与整数的相应定义基本相同.

定义 如果 $f(x)$ 和 $g(x)$ 是 $k[x]$ 中的多项式，其中 k 是域，则 $f(x)$ 和 $g(x)$ 的**公因式**是指多项式 $c(x) \in k[x]$ 满足 $c(x) \mid f(x)$ 和 $c(x) \mid g(x)$. 如果 $f(x)$ 和 $g(x)$ 在 $k[x]$ 中不都为 0，则定义它们的**最大公因式**为次数最高的首一公因式，最大公因式缩记为 gcd. 如果 $f(x) = 0 = g(x)$，则定义它们的 gcd 为 0，常记 $f(x)$ 和 $g(x)$ 的 gcd［由 $f(x)$ 和 $g(x)$ 唯一确定］为 (f,g).

定理 3.31 如果 k 是域，$f(x),g(x) \in k[x]$，则它们的 gcd $d(x)$ 是 $f(x)$ 和 $g(x)$ 的线性组合，即存在 $s(x),t(x) \in k[x]$ 使得

$$d(x) = s(x)f(x) + t(x)g(x).$$

证明概要 与Z中相应结果的证明十分相似. 其实，一旦引入了主理想整环，我们就可以同时证明本定理和Z中相似的结果(见定理 3.57). ■

系 3.32 设 k 是域，$f(x),g(x) \in k[x]$. 一个首一公因式 $d(x)$ 是 gcd 当且仅当 $d(x)$ 被每个公因式整除；即如果 $c(x)$是一个公因式，则 $c(x) \mid d(x)$.

此外，$f(x)$ 和 $g(x)$ 的 gcd 唯一.

证明概要 与命题 1.8 的证明类似. ■

每个多项式 $f(x)$ 可被 u 和 $uf(x)$ 整除，其中 u 是单位. 与素数类似的多项式只有这种平凡的因数.

定义 称整环 R 中的元素 p 为**不可约的**，如果 p 既不是 0 也不是单位，而且它在 R 中的任一因子分解 $p = uv$ 中，u 和 v 必有一个是单位. 称元素 $a,b \in R$ 是**相伴的**，如果存在单位 $u \in R$ 使得 $b = ua$.

例如，素数 $p \in \mathbb{Z}$是不可约元素，$-p$ 也是. 我们现在描述不可约多项式 $p(x) \in k[x]$，其中 k 是域.

命题 3.33 如果 k 是域，则多项式 $p(x) \in k[x]$ 是不可约的当且仅当 $\deg(p) = n \geqslant 1$ 且在 $k[x]$ 中没有形如 $p(x) = g(x)h(x)$ 的因式分解，其中两个因式的次数都小于 n.

证明 首先证明 $h(x) \in k[x]$ 是单位当且仅当 $\deg(h) = 0$. 如果 $h(x)u(x) = 1$，则 $\deg(h) + \deg(u) = \deg(1) = 0$. 因为次数非负，所以有 $\deg(h) = 0$. 反之，如果 $\deg(h) = 0$，则 $h(x)$ 是非零常数，即 $h \in k$. 因 k 是域，故 h 有逆.

如果 $p(x)$ 是不可约的，则它只有这样的因式分解，即 $p(x) = g(x)h(x)$，其中 $g(x)$ 和 $h(x)$ 必有一个是单位；即要么 $\deg(g) = 0$ 要么 $\deg(h) = 0$. 所以 $p(x)$ 不可能有两个因式的次数都比它低的因式分解.

反之，如果 $p(x)$ 不是不可约的，则它有因式分解 $p(x) = g(x)h(x)$，其中 $g(x)$ 和 $h(x)$ 都不是单位；即 $g(x)$ 和 $h(x)$ 的次数都不是 0. 所以 $p(x)$ 有两个因式的次数都比它低的因式分解. ■

135

如果 k 不是域，则不可约多项式的特征不再成立. 例如，$2x+2 = 2(x+1)$ 在$\mathbb{Z}[x]$ 中不是不可约的，即使在任意一个因式分解中，都有一个因式的次数是 0，而另一个是 1（当 k 是域时，单位是非零常数，而对于更一般的系数则不再成立).

因为可除性的定义依赖于所在的环，所以多项式 $p(x) \in k[x]$ 的不可约性依赖于交换环 $k[x]$，从而

也依赖于域 k. 例如，$p(x)=x^2+1$ 在 $\mathbb{R}[x]$ 中是不可约的，但在 $\mathbb{C}[x]$ 中可分解为 $(x+\mathrm{i})(x-\mathrm{i})$. 另一方面，线性多项式 $f(x)$ 总是不可约的 [如果 $f=gh$，则 $1=\deg(f)=\deg(g)+\deg(h)$，从而 g 和 h 之一的次数为 0，而另一个的次数为 $1=\deg(f)$].

系 3.34 设 k 是域，$f(x)\in k[x]$ 是二次或三次多项式，则 $f(x)$ 在 $k[x]$ 中不可约当且仅当 $f(x)$ 在 k 中没有根.

证明概要 如果 $f(x)=g(x)h(x)$ 且 g 和 h 都不是常数，则 $\deg(f)=\deg(g)+\deg(h)$ 蕴涵至少一个因式的次数为 1. ■

易知当 $\deg(f)\geqslant 4$ 时，系 3.34 可能不成立. 例如，在 $\mathbb{R}[x]$ 中考虑多项式 $f(x)=x^4+2x^2+1=(x^2+1)^2$.

例 3.35 (i) 确定 $\mathbb{I}_2[x]$ 中的低次数的不可约多项式.

和通常一样，线性多项式 x 和 $x+1$ 是不可约的.

有四个二次多项式：$x^2, x^2+x, x^2+1, x^2+x+1$（更一般地，在 $\mathbb{I}_p[x]$ 中有 p^n 个 n 次首一多项式，因为 n 个系数 $a_0,\cdots,a_{n-1}$ 的每一个有 p 种选择）. 因为前三个都有根在 $\mathbb{I}_2$ 中，所以不可约二次多项式只有一个.

有 8 个三次多项式，其中 4 个因常数项为 0 所以是可约的，剩下的是

$$x^3+1;\quad x^3+x+1;\quad x^3+x^2+1;\quad x^3+x^2+x+1.$$

因 1 是第一个和第四个的根，所以只有中间的两个是不可约三次多项式.

有 16 个四次多项式，其中 8 个因常数项为 0 所以是可约的. 在 8 个常数项非零的多项式中，有偶数个非零系数的多项式以 1 为根. 现在只有 4 个尚存的多项式 $f(x)$，它们在 $\mathbb{I}_2$ 中没有根，即它们没有线性因式. 如果 $f(x)=g(x)h(x)$，则 $g(x)$ 和 $f(x)$ 必都是不可约二次多项式. 但不可约二次多项式只有一个，就是 x^2+x+1，因而 $(x^2+x+1)^2=x^4+x^2+1$ 是可约的而其他三个四次多项式是不可约的. 下面总结了上面的观察结果.

$\mathbb{I}_2$ 上的低次数的不可约多项式

2 次： x^2+x+1.

3 次： x^3+x+1； x^3+x^2+1.

4 次： x^4+x^3+1； x^4+x+1； $x^4+x^3+x^2+x+1$.

136

(ii) 下面的表是 $\mathbb{I}_3[x]$ 中首一不可约二次和三次多项式. 读者可以验证该表是正确的：先列出所有这种多项式，其中有 6 个首一二次多项式有非零常数项，有 18 个首一三次多项式有非零常数项，然后必须检查哪些多项式以 1 或 -1 为根（用 -1 代替 2 更方便）.

$\mathbb{I}_3$ 上二次、三次不可约首一多项式

2 次： x^2+1； x^2+x-1； x^2-x-1.

3 次： x^3-x+1； x^3+x^2-x+1； x^3-x^2+1；

x^3-x^2+x+1； x^3-x-1； x^3+x^2-1；

x^3+x^2+x-1； x^3-x^2-x-1. ■

易知，如果 $p(x)$ 和 $q(x)$ 都是不可约多项式，则 $p(x)\mid q(x)$ 当且仅当存在单位 u 使得 $q(x)=up(x)$. 另外，如果 $p(x)$ 和 $q(x)$ 都是首一的，则 $p(x)\mid q(x)$ 蕴涵 $p(x)=q(x)$.

引理 3.36 设 k 是域，$p(x),f(x)\in k[x]$，并设 $d(x)=(p,f)$ 是它们的 gcd. 如果 $p(x)$ 是首一不可约多项式，则

$$d(x)=\begin{cases}1 & \text{当 } p(x)\nmid f(x)\\ p(x) & \text{当 } p(x)\mid f(x)\end{cases}$$

证明概要 因 $d(x)\mid p(x)$，有 $d(x)=1$ 或 $d(x)=p(x)$． ■

定理 3.37（欧几里得引理） 设 k 是域，$f(x),g(x)\in k[x]$．如果 $p(x)$ 是 $k[x]$ 中的不可约多项式，且 $p(x)\mid f(x)g(x)$，则要么

$$p(x)\mid f(x) \quad 要么 \quad p(x)\mid g(x).$$

更一般地，如果 $p(x)\mid f_1(x)\cdots f_n(x)$，则有某个 i 使得 $p(x)\mid f_i(x)$．

证明概要 假定 $p\mid fg$ 但 $p\nmid f$．因 p 是不可约的，所以 $(p,f)=1$，从而有多项式 s 和 t 使得 $1=sp+tf$，所以

$$g=spg+tfg.$$

由假设，$p\mid fg$，因而 $p\mid g$． ■

定义 设两个多项式 $f(x),g(x)\in k[x]$，其中 k 是域．如果它们的 gcd 是 1，则称 $f(x)$ 和 $g(x)$ **互素**．

137

系 3.38 设 $f(x),g(x),h(x)\in k[x]$，其中 k 是域，并设 $h(x)$ 和 $f(x)$ 互素．如果 $h(x)\mid f(x)g(x)$，则 $h(x)\mid g(x)$．

证明概要 欧几里得引理的证明也可以用在这里：因 $(h,f)=1$，所以有 $1=sh+tf$，从而 $g=shg+tfg$． ■

定义 如果 k 是域，则有理函数 $f(x)/g(x)\in k(x)$ 称为**有既约形式**，如果 $f(x)$ 和 $g(x)$ 互素．

命题 3.39 假定 k 是域，则每个非零 $f(x)/g(x)\in k(x)$ 都可化为既约形式．

证明概要 如果 $f=df',g=dg'$，其中 $d=(f,g)$，则 f' 和 g' 互素，从而 f'/g' 是既约形式． ■

下一结果使我们可以计算 gcd.

定理 3.40（欧几里得算法） 如果 k 是域，$f(x),g(x)\in k[x]$，则存在计算 gcd (f,g) 的算法，同时可求出一对多项式 $s(x)$ 和 $t(x)$ 使得

$$(f,g)=s(x)f(x)+t(x)g(x).$$

证明 该证明基本上是重复Z 中欧几里得算法的证明．辗转相除如下：

$$\begin{aligned}
g &= q_1 f + r_1\\
f &= q_2 r_1 + r_2\\
r_1 &= q_3 r_2 + r_3\\
&\vdots\\
r_{n-4} &= q_{n-2} r_{n-3} + r_{n-2}\\
r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1}\\
r_{n-2} &= q_n r_{n-1} + r_n\\
r_{n-1} &= q_{n+1} r_n.
\end{aligned}$$

因余式的次数是严格递减的，所以经有限步后该过程必然停止．只要把 r_n 变成首一的，则可断言$d=r_n$ 是 gcd. 从最后往上回代可知 d 是 f 和 g 的公因式．要确定 d 是 gcd，假定 c 是 f 和 g 的任一公因式，则从上往下证明对每个 i 有 $c\mid r_i$. 最后，从下往上倒推便可求出 s 和 t 使得 $d=sf+tg$：

138

$$
\begin{aligned}
r_n &= r_{n-2} - q_n r_{n-1} \\
&= r_{n-2} - q_n(r_{n-3} - q_{n-1}r_{n-2}) \\
&= (1 + q_{n-1})r_{n-2} - q_n r_{n-3} \\
&= (1 + q_{n-1})(r_{n-4} - q_{n-2}r_{n-3}) - q_n r_{n-3} \\
&= (1 + q_{n-1})r_{n-4} - [(1 + q_{n-1})q_{n-2} + q_n]r_{n-3} \\
&\ \vdots \\
&= sf + tg.
\end{aligned}
$$

■

下面是从欧几里得算法得到的一个意外收获.

系 3.41 设 k 是域 K 的子域，从而 $k[x]$ 是 $K[x]$ 的子环. 如果 $f(x),g(x) \in k[x]$，则它们在 $k[x]$ 中的 gcd 等于它们在 $K[x]$ 中的 gcd.

证明 $K[x]$ 中的带余除法给出

$$g(x) = Q(x)f(x) + R(x),$$

其中 $Q(x),R(x) \in K[x]$. 因 $f(x),g(x) \in k[x]$，所以 $k[x]$ 中的带余除法给出

$$g(x) = q(x)f(x) + r(x),$$

其中 $q(x),r(x) \in k[x]$. 但因为 $k[x] \subseteq K[x]$，所以等式 $g(x) = q(x)f(x) + r(x)$ 在 $K[x]$ 中也成立，从而 $K[x]$ 中带余除法的商和余式的唯一性给出 $Q(x) = q(x) \in k[x]$ 和 $R(x) = r(x) \in k[x]$. 因此，在 $K[x]$ 中由欧几里得算法列出的等式和在小环 $k[x]$ 中由欧几里得算法列出的等式是一样的，从而在两个多项式环中得到相同的 gcd. ■

例如，无论在 $\mathbb{R}[x]$ 中还是在 $\mathbb{C}[x]$ 中计算，$x^3 - 2x^2 + x - 2$ 和 $x^4 - 1$ 的 gcd 都是 $x^2 + 1$，尽管复系数有更多的因式.

对于多项式有和算术基本定理类似的结果. 与素数是建造任意整数的“砖块”的意思一样，不可约多项式是构造任意多项式的“砖块”. 为避免句子太长，我们约定“积”可以只有一个因子. 这样，当我们说一个多项式 $f(x)$ 是不可约多项式的积的时候，有可能这个积只有一个因式，也就是说 $f(x)$ 本身是不可约的.

定理 3.42（唯一分解定理） 如果 k 是域，则每个次数 $\geqslant 1$ 的多项式 $f(x) \in k[x]$ 都是非零常数和若干首一不可约多项式的积. 此外，如果 $f(x)$ 有两个这样的因式分解

$$f(x) = ap_1(x)\cdots p_m(x) \quad 和 \quad f(x) = bq_1(x)\cdots q_n(x),$$

即 a 和 b 是非零常数且各个 p 和 q 是首一不可约多项式，则 $a = b, m = n$，且各个 q 经重新标号后可以对一切 i 有 $q_i = p_i$.

139

证明 对 $\deg(f) \geqslant 1$ 用（第二）归纳法证明多项式 $f(x)$ 存在因式分解. 如果 $\deg(f) = 1$，则 $f(x) = ax + c = a(x + a^{-1}c)$. 和每个线性多项式一样，$x + a^{-1}c$ 是不可约的，从而它是不可约多项式的积（在现在用法下的“积”）. 现在假定 $\deg(f) \geqslant 1$. 如果 $f(x)$ 是不可约的且首项系数为 a，则 $f(x) = a(a^{-1}f(x))$，因 $a^{-1}f(x)$ 是首一的，所以结论成立. 如果 $f(x)$ 不是不可约的，则 $f(x) = g(x)h(x)$，其中 $\deg(g) < \deg(f), \deg(h) < \deg(f)$. 由归纳假设，存在因式分解 $g(x) = bp_1(x)\cdots p_m(x), h(x) = cq_1(x)\cdots q_n(x)$，其中各个 p 和 q 是首一不可约多项式. 由此，正如所要的有

$$f(x) = (bc)p_1(x)\cdots p_m(x)q_1(x)\cdots q_n(x),$$

现在对于 $M = \max\{m,n\} \geqslant 1$ 用归纳法证明：如果有等式

$$ap_1(x)\cdots p_m(x) = bq_1(x)\cdots q_n(x),$$

其中 a 和 b 是非零常数且各个 p 和 q 是首一不可约多项式，则 $a=b, m=n$，且各个 q 经重新标号后可以对一切 i 有 $q_i=p_i$. 关于基础步 $M=1$，假设条件给出一个多项式，称为 $g(x)$，它满足 $g(x)=ap_1(x)=bq_1(x)$. 现在因 $p_1(x)$ 是首一的，所以 a 是 $g(x)$ 的首项系数. 同样，因 $q_1(x)$ 也是首一的，所以 b 也是 $g(x)$ 的首项系数，因此 $a=b$，且消去后得 $p_1(x)=q_1(x)$. 关于归纳步，给出的等式表明 $p_m(x) \mid q_1(x)\cdots q_n(x)$. 由多项式的欧几里得引理，存在某个 i 使得 $p_m(x) \mid q_i(x)$. 但 $q_i(x)$ 是首一不可约的，除 1 和它自身外没有首一因式，从而 $q_i(x)=p_m(x)$. 重新标号后，可以假定 $q_n(x)=p_m(x)$. 消去这个因式得 $ap_1(x)\cdots p_{m-1}(x)=bq_1(x)\cdots q_{n-1}(x)$. 根据归纳假设，$a=b$，$m-1=n-1$（因此 $m=n$），且重新标号后对一切 i 有 $q_i=p_i$. ■

设 k 是域，假定存在 $a, r_1, \cdots, r_n \in k$ 使得

$$f(x)=a\prod_{i=1}^{n}(x-r_i).$$

如果 $r_1, \cdots, r_s$（其中 $s \leqslant n$）是 $f(x)$ 的各不相同的根，则组合它的项得

$$f(x)=a(x-r_1)^{e_1}(x-r_2)^{e_2}\cdots(x-r_s)^{e_s},$$

其中 r_j 各不相同且对所有 j，$e_j \geqslant 1$，我们称 e_j 为根 r_j 的**重数**. 因线性多项式总是不可约的，因此唯一因式分解表明根的重数是合理定义的.

尽管有一些方法可以帮助确定一个整数是否是素数，但一般性的问题是非常困难的. 判定一个多项式是否是不可约的也是非常困难的，现在我们提出一些经常使用的有用的方法.

140

我们知道，如果 $f(x) \in k[x]$ 且 r 是 $f(x)$ 在域 k 中的根，则在 $k[x]$ 中有因式分解 $f(x)=(x-r)g(x)$，因此 $f(x)$ 不是不可约的. 在系 3.34 中我们看到它可解决 $k[x]$ 中二次和三次多项式的问题：这些多项式在 $k[x]$ 是不可约的当且仅当它们在 k 中没有根. 对于次数 $\geqslant 4$ 的多项式该结论不再成立.

定理 3.43 设 $f(x)=a_0+a_1x+\cdots+a_nx^n \in \mathbb{Z}[x] \subseteq \mathbb{Q}[x]$. $f(x)$ 的每个有理根 r 形如 b/c，其中 $b \mid a_0, c \mid a_n$.

证明 可以假定 $r=b/c$ 已处于既约形式；即 $(b,c)=1$. 把 r 代入 $f(x)$ 得

$$0=f(b/c)=a_0+a_1b/c+\cdots+a_nb^n/c^n,$$

乘以 c^n 得

$$0=a_0c^n+a_1bc^{n-1}+\cdots+a_nb^n.$$

因此，$a_0c^n=b(-a_1c^{n-1}-\cdots-a_nb^{n-1})$，即 $b \mid a_0c^n$. 因 b 和 c 互素，所以 b 和 c^n 互素，由 $\mathbb{Z}$ 中的欧几里得引理得 $b \mid a_0$. 类似地，$a_nb^n=c(-a_{n-1}b^{n-1}-\cdots-a_0c^{n-1})$，$c \mid a_nb^n$ 和 $c \mid a_n$. ■

定义 称复数 α 为**代数整数**，如果 α 是某首一多项式 $f(x) \in \mathbb{Z}[x]$ 的根.

注意在代数整数的定义中，$f(x) \in \mathbb{Z}[x]$ 是首一的很关键. 每个代数数 z，即每个复数 z 是某多项式 $g(x) \in \mathbb{Q}[x]$ 的根，必定也是某多项式 $h(x) \in \mathbb{Z}[x]$ 的根，只要对 $g(x)$ 系数的分母进行通分.

当然，每个常规整数都是代数整数. 为了区别常规整数和更一般的代数整数，$\mathbb{Z}$ 中的元素可以称为**有理整数**.

系 3.44 如果有理数 z 是代数整数，则 z 必在 $\mathbb{Z}$ 中. 更精确地说，如果 $f(x) \in \mathbb{Z}[x] \subseteq \mathbb{Q}[x]$ 是首一多项式，则 $f(x)$ 的每个有理根是能整除常数项的整数.

证明 如果 $f(x)=a_0+a_1x+\cdots+a_nx^n$ 是首一的，则 $a_n=1$，并可立刻应用定理 3.43. ■

例如，考虑 $f(x)=x^3+4x^2-2x-1\in\mathbb{Q}[x]$．由系 3.34，该三次多项式是不可约的当且仅当它没有有理根．因为 $f(x)$是首一的，$\mathbb{Z}$ 中 -1 的因数只有 ±1，所以可能的有理根只有 ±1．而 $f(1)=2, f(-1)=4$，因此 1 和 -1 都不是根．于是 $f(x)$ 在$\mathbb{Q}$ 中没有根，从而 $f(x)$ 在$\mathbb{Q}[x]$ 中是不可约的．

这个系给出习题1.15(i)一个新的解法．如果 m 是整数而非完全平方数，则多项式 x^2-m 没有整数根，从而$\sqrt{m}$是无理数．其实读者现在可以把它推广到 n 次根：如果 m 是一个非 n 次幂的整数，则$\sqrt[n]{m}$是无理数，因为 x^n-m 的任一有理根必是整数．

[141]

习题

3.28　在$\mathbb{I}_5[x]$中求 x^2-x-2 和 x^3-7x+6 的 gcd，并把它表示为这两个多项式的线性组合．

提示：答案是 $x-2$．

3.29　设 R 是整环．如果 $f(x)\in R[x]$ 的次数为 n，证明 $f(x)$ 在 R 中最多有 n 个根．

提示：用 Frac(R)．

3.30　证明下面的伪码实现了欧几里得算法，该算法可用来在 $\mathbb{I}_3[x]$ 中求 $f(x)$ 和 $g(x)$ 的 gcd，其中 $f(x)=x^2+1, g(x)=x^3+x+1$．

```
Input : g,f
Output : d
d := f;s := g
WHILEs ≠ 0DO
   rem := remainder(h,s)
   h := s
   s := rem
END WHILE
```

3.31　证明欧几里得引理的逆命题．设 k 是域，$f(x)\in k[x]$ 是次数$\geqslant1$ 的多项式．如果 $f(x)$ 一旦整除两个多项式的积必整除其中之一，则 $f(x)$ 是不可约的．

3.32　设 $f(x), g(x)\in R[x]$，其中 R 是整环．如果 $f(x)$ 的首项系数是 R 中的单位，则由带余除法，$g(x)$ 除以 $f(x)$ 得商 $q(x)$ 和余式 $r(x)$．证明 $q(x)$ 和 $r(x)$ 被 $g(x)$ 和 $f(x)$ 唯一确定．

提示：用 Frac(R)．

3.33　设 k 是域，$f(x), g(x)\in k[x]$ 互素．若 $h(x)\in k[x]$，证明 $f(x)\mid h(x)$ 和 $g(x)\mid h(x)$ 蕴涵 $f(x)g(x)\mid h(x)$.

提示：见习题 1.19.

3.34　如果 k 是域且在 k 中 $1+1\neq0$，证明 $\sqrt{1-x^2}\notin k(x)$，其中 $k(x)$ 是有理函数域．

提示：模仿$\sqrt{2}$是无理数的证明．

3.35　(i) 设 R 是域，在 $R[x]$ 中令 $f=p_1^{e_1}\cdots p_m^{e_m}, g=p_1^{\epsilon_1}\cdots p_m^{\epsilon_m}$，其中各个 p_i 是不同的首一不可约多项式，且对一切 $i, e_i, \epsilon_i\geqslant0$（和整数一样，允许出现零指数可以使得两个分解式有相同的不可约因式）．证明 $f\mid g$ 当且仅当对一切 $i, e_i\leqslant\epsilon_i$．

(ii) 用（唯一地）分解为不可约多项式的方法给出求两个多项式的 gcd 和 lcm 的类似于命题 1.17 的公式.

3.36　如果 p 是素数，证明在 $\mathbb{I}_p[x]$ 中恰有 $\frac{1}{3}(p^3-p)$ 个首一不可约三次多项式．（194 页给出了计算 $\mathbb{I}_p[x]$

中首一不可约 n 次多项式的个数的公式.)

3.37 (i) 设 $f(x)=(x-a_1)\cdots(x-a_n)\in k[x]$，其中 k 是域. 证明 $f(x)$ **没有重根**(即所有的 a_i 都是 k 中不同的元素) 当且仅当 $\gcd(f,f')=1$，其中 $f'(x)$ 是 f 的导数.

提示：用习题 3.24.

142 (ii) 证明：如果 $p(x)\in\mathbb{Q}[x]$ 是不可约多项式，则 $p(x)$ 在 $\mathbb{C}$ 中无重根.

提示：系 3.41.

3.38 设 $\zeta=e^{2\pi i/n}$.

(i) 证明

$$x^n-1=(x-1)(x-\zeta)(x-\zeta^2)\cdots(x-\zeta^{n-1}).$$

又，如果 n 是奇数，则

$$x^n+1=(x+1)(x+\zeta)(x+\zeta^2)\cdots(x+\zeta^{n-1}).$$

提示：用系 3.29.

(ii) 对于数 a 和 b，证明

$$a^n-b^n=(a-b)(a-\zeta b)(a-\zeta^2 b)\cdots(a-\zeta^{n-1}b).$$

又，如果 n 是奇数，则

$$a^n+b^n=(a+b)(a+\zeta b)(a+\zeta^2 b)\cdots(a+\zeta^{n-1}b).$$

提示：如果 $b\neq 0$，令 $x=a/b$.

3.5 同态

正如同态用来比较群一样，同态也可用来比较交换环.

定义 如果 A 和 R 是（交换）环，则 **(环) 同态**是指函数 $f:A\to R$ 满足

(i) $f(1)=1$；

(ii) 对一切 $a,a'\in A, f(a+a')=f(a)+f(a)'$；

(iii) 对一切 $a,a'\in A, f(aa')=f(a)f(a')$.

构成双射的同态叫做**同构**. 称交换环 A 和 R 是**同构的**，如果存在同构 $f:A\to R$，记为 $A\cong R$.

例 3.45 (i) 设 R 是整环，记它的分式域为 $F=\mathrm{Frac}(R)$. 在定理 3.13 中，我们说 R 是 F 的子环，但这并不正确，R 甚至不是 F 的子集. 然而，我们的确找到 F 的一个子环 R' 和 R 十分相像，它就是 $R'=\{[a,1]:a\in R\}\subseteq F$. 易知由 $f(a)=[a,1]$ 给出的函数 $f:R\to R'$ 是同构.

(ii) 当把交换环 R 的一个元素“等同”于一个常数多项式的时候［在引理3.16(iii)的证明中]；

143 即把 r 等同于 $(r,0,0,\cdots)$ 的时候，我们把 R 看成 $R[x]$ 的子环. 子集 $R'=\{(r,0,0,\cdots):r\in R\}$ 是 $R[x]$ 的子环，易知由 $f(r)=(r,0,0,\cdots)$ 定义的函数 $f:R\to R'$ 是同构.

(iii) 如果 S 是交换环 R 的子环，则包含映射 $i:S\to R$ 是环同态，因为我们已经强调了 R 的幺元 1 在 S 中.［见习题3.4(iii).］ ■

例 3.46 (i) 复共轭 $z=a+ib\mapsto\bar{z}=a-ib$ 是 $\mathbb{C}\to\mathbb{C}$ 的同态，因为 $\bar{1}=1,\overline{z+w}=\bar{z}+\bar{w}$, $\overline{zw}=\bar{z}\bar{w}$.

(ii) 这里是一个不是同构的环同态的例子. 选取 $m\geqslant 2$，定义 $f:\mathbb{Z}\to\mathbb{I}_m$ 为 $f(n)=[n]$. 注意 f 是满射（但不是单射）.

(iii) 上面的例子可以推广. 如果 R 是交换环，记它的幺元为 ε，则由 $\chi(n)=n\varepsilon$ 定义的函数χ：

$\mathbb{Z}\to R$ 是环同态.[1]

(iv) 设 R 是交换环，$a\in R$. 定义**赋值同态** $e_a:R[x]\to R$ 为 $e_a(f(x))=f(a)$，即如果 $f(x)=\sum r_i x^i$，则 $f(a)=\sum r_i a^i$. 读者可自行验证 e_a 是环同态. ■

环同态 $f:A\to R$ 的某些性质来自 f 作为加法群 A 和 R 之间的同态. 例如，$f(0)=0$，$f(-a)=-f(a)$，以及对一切 $n\in\mathbb{Z}$，$f(na)=nf(a)$.

引理 3.47 如果 $f:A\to R$ 是环同态，则对一切 $a\in A$，

(i) 对一切 $n\geqslant 0$，$f(a^n)=f(a)^n$；

(ii) 如果 a 是单位，则 $f(a)$ 也是单位，且 $f(a^{-1})=f(a)^{-1}$. 事实上，如果 a 是单位，则对一切 $n\geqslant 1$，$f(a^{-n})=f(a)^{-n}$；

(iii) 如果 $f:A\to R$ 是环同态，则

$$f(\mathrm{U}(A))\leqslant \mathrm{U}(R),$$

其中 $U(A)$ 是 A 的单位群. 如果 f 是同构，则

$$\mathrm{U}(A)\cong \mathrm{U}(R).$$

证明概要 (i) 对 $n\geqslant 0$ 用归纳法.

(ii) 如果 $ab=1$，则 $1=f(ab)=f(a)f(b)$. 后一个陈述来自对 $n\geqslant 1$ 用归纳法.

(iii) 由 (ii) 立得. ■　[144]

命题 3.48 如果 R 和 S 是交换环，$\varphi:R\to S$ 是环同态，则存在由

$$\varphi^*: r_0+r_1x+r_2x^2+\cdots\mapsto \varphi(r_0)+\varphi(r_1)x+\varphi(r_2)x^2+\cdots$$

给出的环同态 $\varphi^*:R[x]\to S[x]$.

证明概要 显然 φ^* 是合理定义的，经简单计算可以证明它是环同态. ■

定义 如果 $f:A\to R$ 是环同态，则它的**核**是指

$$\ker f=\{a\in A \text{ 满足 } f(a)=0\},$$

它的**象**是指

$$\mathrm{im} f=\{r\in R: \text{存在 } a\in A \text{ 使得 } r=f(a)\}.$$

注意，如果忘掉它们的乘法，则环 A 和 R 是加法阿贝尔群，上面的定义和群论中的定义一致.

设 k 是交换环，$a\in k$，和例3.46(iv)一样，考虑赋值同态 $e_a:k[x]\to k$ 把 $f(x)$ 发送到 $f(a)$. 现在 e_a 恒为满射，因为如果 $b\in k$，则 $b=e_a(f)$，其中 $f(x)=x-a+b$. 根据定义，$\ker e_a$ 由满足 $g(a)=0$ 的那些多项式 $g(x)$ 组成，即 $\ker e_a$ 由 $k[x]$中一切以 a 为根的多项式组成.

群同态的核不只是一个子群，它还是正规子群；即它对于所在群中的任一元素的共轭封闭. 类似地，如果 R 不是零环，则环同态 $f:A\to R$ 的核几乎是一个子环 [$\ker f$ 不是子环，因为它从不包含 1：$f(1)=1\neq 0$]，而且我们将看到，它乘以所在环中的任一元素是封闭的.

定义 交换环 R 的**理想**是指 R 的子集 I 满足

(i) $0\in I$；

(ii) 如果 $a,b\in I$，则 $a+b\in I$；[2]

---

[1] 回顾如果 $a\in R$ 且 n 是正整数，则 na 是乘法记号 a^n 的加法翻版，即 na 是 n 个 a 的和.

[2] 和子环的定义相比，这里只需假定 $a+b\in I$ 而取代 $a-b\in I$. 如果 I 是理想且 $b\in I$，则 $(-1)b\in I$，从而 $a-b=a+(-1)b\in I$.

(iii) 如果 $a\in I$，$r\in R$，则 $ra\in I$.

环 R 本身和只有一个元素 0 组成的子集（记为 $\{0\}$）恒为交换环 R 的理想．称理想 $I\neq R$ 为**真理想**．

例 3.49 如果 b_1，b_2，…，b_n 在 R 中，则一切线性组合的集合

145

$$I=\{r_1b_1+r_2b_2+\cdots+r_nb_n : r_i\in R,\text{对一切 }i\}$$

是 R 中的理想．此时记 $I=(b_1,b_2,\cdots,b_n)$，并称 I 是由 $b_1,b_2,\cdots,b_n$ **生成的理想**．特别是如果 $n=1$，则

$$I=(b)=\{rb : r\in R\}$$

是 R 中的理想，(b) 由 b 的一切倍数组成，称为由 b 生成的**主理想**．注意 R 和 $\{0\}$ 恒为主理想：$R=(1),\{0\}=(0)$．在$\mathbb{Z}$中偶整数形成主理想 (2)． ■

命题 3.50 如果 $f:A\to R$ 是环同态，则 $\ker f$ 是 A 中的理想，$\operatorname{im} f$ 是 R 的子环．此外，如果 A 和 R 都不是零环，则 $\ker f$ 是真理想．

证明概要 $\ker f$ 是 A 的加法子群．如果 $u\in\ker f,a\in A$，则 $f(au)=f(a)f(u)=f(a)\cdot 0=0$，因此 $\ker f$ 是理想．如果 R 不是零环，则 $1\neq 0$，由于在 R 中 $f(1)=1\neq 0$，因此幺元 $1\in A$ 不在 $\ker f$ 中，从而 $\ker f$ 是真理想．容易验证 $\operatorname{im} f$ 是 R 的子环． ■

例 3.51 (i) 如果交换环 R 的理想 I 包含 1，则对每个 $r\in R$，I 包含 $r=r1$，从而 $I=R$．其实如果 I 包含单位 u，则 $I=R$，因为此时 I 包含 $u^{-1}u=1$．

(ii) 由 (i)，如果 R 是域，则 R 中只有 $\{0\}$ 和 R 自身是理想：如果 $I\neq\{0\}$，则 I 包含某个非零元素，而域中的每个非零元素都是单位．

反之，假定 R 是非零交换环，且它的理想只有 $\{0\}$ 和 R 自身．如果 $a\in R$ 且 $a\neq 0$，则因主理想 $(a)\neq\{0\}$，所以有 $(a)=R$ 且 $1\in R=(a)$．于是存在 $r\in R$ 使得 $1=ra$；即 a 在 R 中有逆，所以 R 是域． ■

命题 3.52 环同态 $f:A\to R$ 是单射当且仅当 $\ker f=\{0\}$．

证明概要 因为 f 是从加法群 A 到加法群 R 的同态，所以结论由群同态的相应结果而得． ■

系 3.53 如果 $f:k\to R$ 是环同态，其中 k 是域而 R 是非零环，则 f 是单射．

证明 k 中只有真理想 $\{0\}$． ■

定理 3.54 如果 k 是域，则 $k[x]$ 中的每个理想 I 都是主理想．此外，如果 $I\neq\{0\}$，则存在首一多项式生成 I.

证明概要 如果 k 是域，则 $k[x]$ 是定理 3.60 中欧几里得环的一个例子，我们将证明在欧几里得环中每个理想都是主理想． ■

146

定义 整环 R 称为**主理想整环**，如果 R 中的每个理想都是主理想．该名称常缩写为 PID.

例 3.55 (i) 整数环是 PID.

(ii) 由例3.51(ii)，每个域都是 PID.

(iii) 如果 k 是域，则由定理 3.54，多项式环 $k[x]$是 PID.

(iv) 除了$\mathbb{Z}$和 $k[x]$（其中 k 是域）之外，还存在具有带余除法的环，这种环称为欧几里得环，它们也是 PID，我们将在下一节考虑这种环． ■

在任意交换环中，理想并不都是主理想．

例 3.56 设 $R=\mathbb{Z}[x]$ 是$\mathbb{Z}$上一切多项式的交换环．易知一切带有偶常数项的多项式的集合 I 是$\mathbb{Z}[x]$ 中的理想．我们证明 I 不是主理想．

假设存在 $d(x) \in \mathbb{Z}[x]$ 使得 $I = (d(x))$．常数 $2 \in I$，从而有 $f(x) \in \mathbb{Z}[x]$ 使得 $2 = d(x)f(x)$. 因积的次数是因式次数的和，所以 $0 = \deg(2) = \deg(d) + \deg(f)$．由于次数非负，因此 $\deg(d) = 0$[即 $d(x)$ 是非零常数]．这里常数是整数，$d(x)$ 可能是 ± 1 和 ± 2. 假设 $d(x) = \pm 2$．因 $x \in I$，故有 $g(x) \in \mathbb{Z}[x]$ 使得 $x = d(x)g(x) = \pm 2g(x)$，但右边的每个系数都是偶数，而左边 x 的系数是 1. 这个矛盾给出 $d(x) = \pm 1$．由例3.51(ⅱ)，$I = \mathbb{Z}[x]$，这又是矛盾．所以这样的 $d(x)$ 不存在，即理想 I 不是主理想． ■

一些通常的定义一旦推广以后，某些在 $\mathbb{Z}$ 中成立的定理可以引入 PID 中．因子的概念已经得到了推广．

定义 交换环 R 中的元素 δ 称为元素 $\alpha,\beta \in R$ 的**最大公因子**，即 gcd，如果

(ⅰ) δ 是 α 和 β 的公因子；

(ⅱ) 如果 γ 是 α 和 β 的任一公因子，则 $\gamma \mid \delta$.

当最大公因子存在的时候，它并不一定唯一．例如，如果 c 是 f 和 g 的最大公因子，易知对任一单位 $u \in R$，uc 也是最大公因子．特别是在 $R = \mathbb{Z}$ 的情形，我们要求 gcd 是正数从而获得唯一性．如果 $R = k[x]$，其中 k 是域，则要求 gcd 是首一的以获得唯一性． 147

注 设 R 是 PID，$\pi,\alpha \in R$，且 π 是不可约的．π 和 α 的 gcd δ 是 π 的因子，因此 $\pi = \delta\varepsilon$. π 的不可约性使得 δ 或 ε 必须是单位．现在 $\alpha = \delta\beta$. 如果 δ 不是单位，则 ε 是单位，从而

$$\alpha = \delta\beta = \pi\varepsilon^{-1}\beta;$$

即 $\pi \mid \alpha$. 由此可知，如果 $\pi \nmid \alpha$，则 δ 是单位；即 1 是 π 和 α 的 gcd.

有一个整环的例子，其中有一对元素没有 gcd，见习题 3.60.

定理 3.57 设 R 是 PID.

(ⅰ) 每对 $\alpha,\beta \in R$ 都有 gcd δ，它是 α 和 β 的线性组合：

$$\delta = \sigma\alpha + \tau\beta,$$

其中 $\sigma,\tau \in R$.

(ⅱ) 如果不可约元素 $\pi \in R$ 整除乘积 $\alpha\beta$，则要么 $\pi \mid \alpha$ 要么 $\pi \mid \beta$.

证明 (ⅰ) 可以假定 α 和 β 至少一个非零（否则，gcd 是 0，结论显然成立）．考虑一切线性组合的集合 I：

$$I = \{\sigma\alpha + \tau\beta : \sigma,\tau \in R\}.$$

现在 α 和 β 在 I 中（取 $\sigma = 1, \tau = 0$ 或者两者对调）．容易验证 I 是 R 中的理想，因 R 是 PID，存在 $\delta \in I$ 使得 $I = (\delta)$．我们断言 δ 是 α 和 β 的 gcd.

因 $\alpha \in I = (\delta)$，所以有某个 $\rho \in R$ 使得 $\alpha = \rho\delta$；即 δ 是 α 的因子．同样，δ 是 β 的因子，所以 δ 是 α 和 β 的公因子．

因 $\delta \in I$，所以它是 α 和 β 的线性组合：存在 $\sigma,\tau \in R$ 使得

$$\delta = \sigma\alpha + \tau\beta.$$

最后，如果 γ 是 α 和 β 的任一公因子，则 $\alpha = \gamma\alpha', \beta = \gamma\beta'$，因 $\delta = \sigma\alpha + \tau\beta = \gamma(\sigma\alpha' + \tau\beta')$，$\gamma$ 整除 δ. 由此可知 δ 是 gcd.

(ⅱ) 如果 $\pi \mid \alpha$，则结论已经成立．如果 $\pi \nmid \alpha$，则上面的注说 1 是 π 和 α 的 gcd，于是存在元素 $\sigma,\tau \in R$ 使得 $1 = \sigma\pi + \tau\alpha$，由此

$$\beta = \sigma\pi\beta + \tau\alpha\beta.$$

因 $\pi \mid \alpha\beta$，从而正如所要的有 $\pi \mid \beta$. ■

例 3.58 如果 I，J 是交换环 R 中的理想，我们现在证明 $I \cap J$ 也是 R 中的理想. 因 $0 \in I, 0 \in J$，所以有 $0 \in I \cap J$. 如果 $a,b \in I \cap J$，则因 I,J 都是理想，故 $a-b \in I, a-b \in J$，从而 $a-b \in I \cap J$. 如果 $a \in I \cap J, r \in R$，则 $ra \in I, ra \in J$，因此 $ra \in I \cap J$. 所以 $I \cap J$ 是理想. 稍作修改，这一论证可以证明 R 中任一理想族的交也是 R 中的理想. ■

148

定义 如果 f 和 g 是交换环 R 的元素，则元素 $m \in R$ 满足 $f \mid m, g \mid m$，称为 f 和 g 的**公倍数**. 如果 f 和 g 在 R 中不都为 0，则定义它们的**最小公倍数**(缩写为 lcm) 为对每个公倍数 m 满足 $c \mid m$ 的公倍数 c. 如果 $f=0=g$，则定义它们的 lcm 为 0. f 和 g 的 lcm 常记为 $[f,g]$.

当最小公倍数存在的时候，它未必唯一. 例如，如果 c 是 f 和 g 的最小公倍数，则对任一单位 $u \in R$, uc 也是 f 和 g 的最小公倍数. 特别是在 $R=\mathbb{Z}$ 的情形，我们要求 lcm 是正数以获得其唯一性. 如果 $R=k[x]$，其中 k 是域，则要求 lcm 是首一的以获得唯一性.

习题

3.39 (i) 设 $\varphi: A \to R$ 是同构，并设 $\psi: R \to A$ 是它的逆. 证明 ψ 也是同构.

(ii) 证明两个同态（同构）的复合也是同态（同构）.

(iii) 证明 $A \cong R$ 在所有交换环的类上定义了一个等价关系.

3.40 设 R 是交换环，$\mathcal{F}(R)$ 是一切函数 $f: R \to R$ 连同点态运算的交换环.

(i) 证明 R 同构于由一切常数函数组成的 $\mathcal{F}(R)$ 的子环.

(ii) 设 $f(x) \in R[x]$，定义 $\varphi_f: R \to R$ 为 $r \mapsto f(r)$ [由此，φ_f 是相应于 $f(x)$ 的多项式函数]. 证明由 $\varphi(f(x)) = \varphi_f$ 定义的函数 $\varphi: R[x] \to \mathcal{F}(R)$ 是环同态.

(iii) 证明：如果 R 是无限域，则 φ 是单射.

3.41 设 I 和 J 是交换环 R 中的非零理想. 证明：如果 R 是整环，则 $I \cap J \neq \{0\}$.

3.42 设 R 是交换环. 证明由

$$\varepsilon: a_0 + a_1 x + a_2 x + \cdots + a_n x^n \mapsto a_0$$

定义的函数 $\varepsilon: R[x] \to R$ 是同态. 用多项式的根描述 $\ker\varepsilon$.

3.43 (i) 设 R 和 S 都是交换环，$\varphi: R \to S$ 是环同态. 如果 $s \in S$，证明存在一个唯一的环同态 $\tilde{\varphi}: R[x] \to S$，使得对一切 $r \in R$ 有 $\tilde{\varphi}(r) = \varphi(r)$，以及 $\tilde{\varphi}(x) = s$.

(ii) 如果 R 是交换环，$c \in R$. 证明由 $f(x) \mapsto f(x+c)$ 定义的函数 $\varphi: R[x] \to R[x]$ 是同构. 更详细地说，$\varphi(\sum_i s_i x^i) = \sum_i s_i (x+c)^i$.

提示：证明简单但计算较长.

3.44 (i) 证明有四个元素的域 F（见习题 3.14）和 $\mathbb{I}_4$ 不是同构的交换环.

(ii) 证明恰有四个元素的任两个域是同构的.

提示：先证明 $1+1=0$，然后证明非零元素在乘法下形成 3 阶循环群.

3.45 (i) 证明每个元素 $a \in \mathbb{I}_p$ 都有 p 次根（即存在 $b \in \mathbb{I}_p$ 使得 $a=b^p$）.

(ii) 设 k 是包含 $\mathbb{I}_p$ 并把它作为子域的域 [例如，$k=\mathbb{I}_p(x)$]. 证明对每个正整数 n，由 $\varphi(a)=a^{p^n}$ 给出的函数 $\varphi_n: k \to k$ 是环同态.

149

3.46 如果 R 是域，证明 $R \cong \mathrm{Frac}(R)$. 更精确地说，是要证明例3.45(i)中的同态 $f: R \to \mathrm{Frac}(R)$（也就是 $r \mapsto [r,1]$）是同构.

3.47 (i) 如果 A 和 R 是整环，$\varphi: A \to R$ 是环同构，证明

$$[a,b] \mapsto [\varphi(a), \varphi(b)]$$

是环同构 $\mathrm{Frac}(A) \to \mathrm{Frac}(R)$.

(ii) 如果域 k 包含 $\mathbb{Z}$ 的一个同构象作为子环，证明 k 必包含 $\mathbb{Q}$ 的一个同构象.

(iii) 设 R 是整环，$\varphi: R \to k$ 是单射环同态，其中 k 是域. 证明存在唯一的环同态 $\Phi: \mathrm{Frac}(R) \to k$ 扩张 φ；即 $\Phi | R = \varphi$.

3.48 设 R 是整环，它具有分式域 $F = \mathrm{Frac}(R)$.

(i) 证明 $\mathrm{Frac}(R[x]) \cong F(x)$.

(ii) 证明 $\mathrm{Frac}(R[x_1 x_2, \cdots, x_n]) \cong F(x_1, x_2, \cdots, x_n)$ (见 129 页).

3.49 (i) 如果 R 和 S 是交换环，证明它们的直积 $R \times S$ 也是交换环，其中 $R \times S$ 中的加法和乘法由“坐标形态”的加法和乘法定义：

$$(r,s) + (r',s') = (r+r', s+s'), (r,s)(r',s') = (rr', ss').$$

(ii) 如果 m 和 n 互素，证明作为环有 $\mathbb{I}_{mn} \cong \mathbb{I}_m \times \mathbb{I}_n$.

提示：见定理 2.81.

(iii) 如果 R 和 S 都是非零环，证明 $R \times S$ 不是整环.

(iv) 证明 $R \times \{0\}$ 是 $R \times S$ 中的理想.

(v) 证明 $R \times \{0\}$ 环同构于 R，但它不是 $R \times S$ 的子环.

3.50 (i) 如果 R 和 S 都是非零交换环，证明

$$U(R \times S) = U(R) \times U(S),$$

其中 $U(R)$ 是 R 的单位群.

提示：证明 (r,s) 是 $R \times S$ 的单位当且仅当 r 是 R 中的单位而 s 是 S 中的单位.

(ii) 用 (i) 重做习题 2.65.

(iii) 用 (i) 给出系 2.83 的另一个证明.

3.51 设 F 是形如

$$A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

的一切 2×2 实数矩阵的集合，证明 F 是域（运算是矩阵加法和矩阵乘法），并证明存在同构 $\varphi: F \to \mathbb{C}$ 使得 $\det(A) = \varphi(A)\overline{\varphi(A)}$.

提示：定义 $\varphi: F \to \mathbb{C}$ 为 $\varphi(A) = a + ib$.

3.52 如果 k 是域，$[f,g]$ 表示首一多项式 $f(x), g(x) \in k[x]$ 的 lcm，证明

$$[f,g](f,g) = fg.$$

提示：见习题 1.26. 由定义，lcm 是首一的.

150

3.53 如果 R 是 PID，$a, b \in R$，证明它们的 lcm 存在.

3.54 (i) 如果 k 是域，证明形式幂级数环 $k[[x]]$ 是 PID.

提示：如果 I 是非零理想，选取阶最小的 $\tau \in I$. 用习题 3.27 证明 $I = (\tau)$.

(ii) 证明 $k[[x]]$ 中的每个非零理想等于 (x^n)，其中 $n \geq 0$.

3.55 如果 k 是域. 证明 $k[x,y]$ 中的理想 (x,y) 不是主理想（见 129 页）.

3.56 对 $m \geq 1$，证明 $\mathbb{I}_m$ 中的每个理想都是主理想.（如果 m 是合数，则 $\mathbb{I}_m$ 不是 PID，因为它不是整环.）

3.6 欧几里得环

存在 $\mathbb{Z}$ 和 $k[x]$（k 是域）之外具有带余除法的环. 我们特别举出一个这样的环的例子，它的商

和余式不唯一．下面从推广$\mathbb{Z}$和$k[x]$共有的一个性质开始．

定义 **欧几里得环**是指整环R，它在R上配置了函数

$$\partial: R-\{0\} \to \mathbb{N},$$

使得

(i) 对一切$f, g \in R$且$f, g \neq 0, \partial(f) \leqslant \partial(fg)$；

(ii) 对一切$f, g \in R$且$f \neq 0$，存在$q, r \in R$满足

$$g = qf + r,$$

其中$r=0$或$\partial(r) < \partial(f)$．该函数称为**次数函数**．

注意，如果R有一个恒等于0的次数函数∂，则条件（ii）始终迫使$r=0$，取$g=1$表明此时R是域．

例 3.59 （i）整数$\mathbb{Z}$是欧几里得环，次数函数$\partial(m)=|m|$．在$\mathbb{Z}$中有

$$\partial(mn)=|mn|=|m||n|=\partial(m)\partial(n).$$

（ii）当k是域时，整环$k[x]$是欧几里得环，次数函数是通常的非零多项式的次数．在$k[x]$中有

$$\begin{aligned}\partial(fg) &= \deg(fg)\\ &= \deg(f)+\deg(g)\\ &= \partial(f)+\partial(g).\end{aligned}$$

151

因在$\mathbb{Z}$中$\partial(mn)=\partial(m)\partial(n)$，乘积次数的状况并没有被定义次数函数的公理所确定．如果次数函数∂是可乘的，即如果

$$\partial(fg)=\partial(f)\partial(g),$$

则称∂为**范数**．

（iii）高斯整数[⊖]$\mathbb{Z}[i]$形成欧几里得环，它的次数函数

$$\partial(a+bi)=a^2+b^2$$

是范数．证明$\mathbb{Z}[i]$是欧几里得环的一个原因是为了说明它是PID，从而它的元素可以唯一地分解为不可约元素的乘积．高斯运用这一事实证明：如果奇素数p是两个平方数的和，比如$p=a^2+b^2$，其中a，b是自然数，则a，b这对数是唯一的（见定理3.66）．

为证明∂是可乘的次数函数，首先注意，如果$\alpha=a+bi$，则

$$\partial(\alpha)=\alpha\bar{\alpha},$$

其中$\bar{\alpha}=a-bi$是α的复共轭．因为

$$\partial(\alpha\beta)=\alpha\beta\overline{\alpha\beta}=\alpha\beta\bar{\alpha}\bar{\beta}=\alpha\bar{\alpha}\beta\bar{\beta}=\partial(\alpha)\partial(\beta);$$

所以对一切$\alpha,\beta\in\mathbb{Z}[i], \partial(\alpha\beta)=\partial(\alpha)\partial(\beta)$．其实由系1.31，对于一切$\alpha,\beta\in\mathbb{Q}[i]=\{x+yi: x,y\in\mathbb{Q}\}$也成立．

现在我们证明∂满足次数函数的第一个性质．如果$\beta=c+id\in\mathbb{Z}[i]$且$\beta\neq0$，则因为$\partial(\beta)=c^2+d^2$是正整数，故

$$1\leqslant\partial(\beta),$$

由此，如果$\alpha,\beta\in\mathbb{Z}[i]$且$\beta\neq0$，则

$$\partial(\alpha)\leqslant\partial(\alpha)\partial(\beta)=\partial(\alpha\beta).$$

⊖ 所以称为高斯整数是因为高斯默认了$\mathbb{Z}[i]$和它的范数∂，以用来研究双二次的残数．

再证明 ∂ 也满足第二个性质．给定 $\alpha,\beta\in\mathbb{Z}[i]$ 且 $\beta\neq 0$，把 α/β 看作 $\mathbb{C}$ 中的一个元素．将分母有理化得 $\alpha/\beta=\alpha\bar{\beta}/\beta\bar{\beta}=\alpha\bar{\beta}/\partial(\beta)$，从而

$$\alpha/\beta=x+yi,$$

其中 $x,y\in\mathbb{Q}$．记 $x=a+u,y=b+v$，其中 $a,b\in\mathbb{Z}$ 分别是 x,y 的整数逼近，于是 $|u|,|v|\leqslant\frac{1}{2}$．（如果 x 或 y 形如 $m+\frac{1}{2}$，其中 m 是整数，则最近整数可在两个数中选一个：$x=m+\frac{1}{2}$ 或 $x=(m+1)-\frac{1}{2}$．对 x 或 y 形如 $m-\frac{1}{2}$ 也有同样的选择．）由此

$$\alpha=\beta(a+bi)+\beta(u+vi).$$

152

注意 $\beta(u+vi)\in\mathbb{Z}[i]$，因为它等于 $\alpha-\beta(a+bi)$．最后，我们有

$$\partial(\beta(u+vi))=\partial(\beta)\partial(u+vi),$$

从而如果 $\partial(u+vi)<1$，则 ∂ 是一个次数函数．这个条件是成立的，因为不等式 $|u|\leqslant\frac{1}{2},|v|\leqslant\frac{1}{2}$ 给出 $u^2\leqslant\frac{1}{4},v^2\leqslant\frac{1}{4}$，于是 $\partial(u+ui)=u^2+v^2\leqslant\frac{1}{4}+\frac{1}{4}=\frac{1}{2}<1$. 所以 $\partial(\beta(u+vi))<\partial(\beta)$，从而 $\mathbb{Z}[i]$ 是欧几里得环，它的次数函数是范数．

我们现在证明商和余数可以不唯一（由于前面提到的选择）．例如，令 $\alpha=3+5i,\beta=2$，则 $\alpha/\beta=\frac{3}{2}+\frac{5}{2}i$，几种选择是

$$a=1,u=\frac{1}{2}\quad\text{或}\quad a=2,u=-\frac{1}{2};$$

$$b=2,v=\frac{1}{2}\quad\text{或}\quad b=3,v=-\frac{1}{2}.$$

在 $\mathbb{Z}[i]$ 中 $3+5i$ 除以 2 有四个商和余数，每个余数（例如，$1+i$）的次数为 $2<4=\partial(2)$：

$$\begin{aligned}3+5i&=2(1+2i)+(1+i);\\&=2(1+3i)+(1-i);\\&=2(2+2i)+(-1+i);\\&=2(2+3i)+(-1-i).\end{aligned}$$

■

定理 3.60　*每个欧几里得环都是 PID.*

证明　设 I 是 R 中的理想．如果 $I=\{0\}$，则 $I=(0)$ 是主理想，所以我们可以假定 $I\neq(0)$．由最小整数公理，I 中一切非零元素的次数的集合有最小元素，比如 n. 选取 $d\in I$ 满足 $\partial(d)=n$．显然 $(d)\subseteq I$，因此只需证明反包含．如果 $a\in I$，则有 $q,r\in R$ 使得 $a=qd+r$，其中 $r=0$ 或 $\partial(r)<\partial(d)$. 而 $r=a-qd\in I$，因此 d 的次数最小蕴涵 $r=0$．所以 $a=qd\in(d)$，从而 $I=(d)$．■

系 3.61　*高斯整数环 $\mathbb{Z}[i]$ 是主理想整环．*

定理 3.60 的逆不成立：由下面的例子可知，存在不是欧几里得环的 PID.

例 3.62　在代数数论中证明了环

$$R=\{a+b\alpha : a,b\in\mathbb{Z}\}$$

是 PID，其中 $\alpha=\frac{1}{2}(1+\sqrt{-19})$［$R$ 是二次数域 $\mathbb{Q}(\sqrt{-19})$ 中的代数整数环］．1949 年，T. S. Motzkin 通过证明 R 不具备欧几里得环的某个不牵涉次数函数的性质证明了 R 不是欧几里得环．

■　153

定义 整环 R 中的元素 u 称为**万能旁因子**，如果 u 不是单位且对每个 $x \in R$，或者 $u \mid x$，或者存在单位 $z \in R$ 使得 $u \mid (x+z)$.

命题3.63 如果 R 是欧几里得环但不是域，则 R 有万能旁因子.

证明 定义

$$S = \{\partial(v) : v \neq 0 \text{ 且 } v \text{ 不是单位}\},$$

其中 ∂ 是 R 上的次数函数. 因假设 R 不是域，所以 S 是自然数的非空子集. 根据最小整数公理，S 有最小元素，比如 $\partial(u)$. 我们断言 u 是一个万能旁因子. 如果 $x \in R$，则有元素 q，r 使得 $x = qu + r$，其中 $r = 0$ 或 $\partial(r) < \partial(u)$. 如果 $r = 0$，则 $u \mid x$；如果 $r \neq 0$，则 r 必是单位，否则便与 $\partial(u)$ 是 S 中的最小数矛盾. 由此证明了 u 是一个万能旁因子. ■

Motzkin 证明环 $\{a + b\alpha : a,b \in \mathbb{Z}\}\left(\text{其中 } \alpha = \frac{1}{2}(1+\sqrt{-19})\right)$ 没有万能旁因子，由此推出这个 PID 不是欧几里得环. 详细内容读者可参考 K. S. Williams 的 "Note on Non-euclidean Principal Ideal Domians," *Math. Mag.* 48 (1975)，176～177 页. ■

高斯整数中的单位是什么?

命题3.64 (i) 设 R 是欧几里得环，但 R 不是域. 如果次数函数 ∂ 是范数，则 α 是单位当且仅当 $\partial(\alpha) = 1$.

(ii) 设 R 是欧几里得环，但 R 不是域. 如果次数函数 ∂ 是范数且 $\partial(\alpha) = p$，其中 p 是素数，则 α 不可约.

(iii) 高斯整数环 $\mathbb{Z}[i]$ 中的单位只有 ± 1 和 $\pm i$.

证明 (i) 因 $1^2 = 1$，故有 $\partial(1)^2 = \partial(1)$，从而 $\partial(1) = 0$ 或 $\partial(1) = 1$. 如果 $\partial(1) = 0$，则对所有 $a \in R$, $\partial(a) = \partial(1a) = \partial(1)\partial(a) = 0$. 但 R 不是域，因此 ∂ 不恒为零. 由此可知 $\partial(1) = 1$.

如果 $\alpha \in R$ 是单位，则存在 $\beta \in R$ 使得 $\alpha\beta = 1$. 所以 $\partial(\alpha)\partial(\beta) = 1$. 因 ∂ 的值是非负整数，从而 $\partial(\alpha) = 1$.

关于逆命题，我们先证明 R 中没有 $\partial(\beta) = 0$ 的元素 $\beta \in R$. 如果存在这样的元素，则带余除法给出 $1 = q\beta + r$，其中 $q, r \in R$ 且 $r = 0$ 或 $\partial(r) < \partial(\beta) = 0$，不等式不可能出现，所以 $r = 0$，即 β 是单位. 但我们已经证明，如果 β 是单位，则 $\partial(\beta) = 1$，这与 $\partial(\beta) = 0$ 矛盾.

现在假定 $\partial(\alpha) = 1$. 带余除法给出 $q, r \in R$ 使得

154

$$\alpha = q\alpha^2 + r,$$

其中 $r = 0$ 或 $\partial(r) < \partial(\alpha^2)$. 因为 $\partial(\alpha^2) = \partial(\alpha)^2 = 1$，因而或者 $r = 0$ 或者 $\partial(r) = 0$. 但我们已经知道 $\partial(r) = 0$ 不可能出现，从而 $r = 0$, $\alpha = q\alpha^2$. 由此 $1 = q\alpha$，从而 α 是单位.

(ii) 相反，如果 $\alpha = \beta\gamma$，其中 β, γ 都不是单位，则 $p = \partial(\alpha) = \partial(\beta)\partial(\gamma)$. 因 p 是素数，所以 $\partial(\beta) = 1$ 或 $\partial(\gamma) = 1$. 由 (i)，β 和 γ 中有一个是单位，即 α 是不可约的.

(iii) 如果 $\alpha = a + bi \in \mathbb{Z}[i]$ 是单位，则 $1 = \partial(\alpha) = a^2 + b^2$，该式成立当且仅当 $a^2 = 1$ 且 $b^2 = 0$，或 $a^2 = 0$ 且 $b^2 = 1$，即 $\alpha = \pm 1$ 或 $\alpha = \pm i$. ■

如果 n 是奇数，则 $n \equiv 1 \bmod 4$ 或 $n \equiv 3 \bmod 4$，由此奇素数分成两类. 例如，5,13,17 对 mod4 与 1 同余，而 3,7,11 对 mod4 与 3 同余.

引理3.65 如果 p 是素数且 $p \equiv 1 \bmod 4$，则存在整数 m 使得

$$m^2 \equiv -1 \bmod p.$$

证明 令 $G=(\mathbb{I}_p)^\times$ 为 $\mathbb{I}_p$ 中非零元素的乘法群，则 $|G|=p-1\equiv 0 \bmod 4$，即 4 是 $|G|$ 的因数．由命题 2.78，G 包含一个 4 阶子群 S. 根据习题 2.36，S 或者是循环群，或者对一切 $a\in S$ 有 $a^2=1$．然而，因为 $\mathbb{I}_p$ 是域，它不可能包含二次多项式 x^2-1 的四个根，所以 S 是循环群[㊀]，比如 $S=\langle[m]\rangle$，其中 $[m]$ 是 $m \bmod p$ 的同余类．因 $[m]$ 的阶为 4，所以有 $[m^4]=[1]$．此外，$[m^2]\neq[1]$（否则 $[m]$ 的阶 $\leqslant 2<4$）．因为 $[-1]$ 是 S 中唯一的 2 阶元素，从而 $[m^2]=[-1]$．所以 $m^2\equiv -1 \bmod p$. ■

定理 3.66（费马[㊁]二平方和定理） 奇素数是两平方数的和，

$$p=a^2+b^2,$$

当且仅当 $p\equiv 1 \bmod 4$，其中 a 和 b 是整数．

证明 假定 $p=a^2+b^2$．因 p 是奇数，所以 a 和 b 的奇偶性不同，比如 a 是偶数，b 是奇数．从而 $a=2m, b=2n+1$，且

$$p=a^2+b^2=4m^2+4n^2+4n+1\equiv 1 \bmod 4.$$

反之，假定 $p\equiv 1 \bmod 4$．由引理，存在整数 m 使得

$$p\mid(m^2+1).$$

在 $\mathbb{Z}[\mathrm{i}]$ 中有因式分解 $m^2+1=(m+\mathrm{i})(m-\mathrm{i})$，从而

$$\text{在 } \mathbb{Z}[\mathrm{i}] \text{ 中有 } p\mid(m+\mathrm{i})(m-\mathrm{i}).$$

如果在 $\mathbb{Z}[\mathrm{i}]$ 中 $p\mid(m\pm\mathrm{i})$，则存在整数 u 和 v 使得 $m\pm\mathrm{i}=p(u+\mathrm{i}v)$．比较虚部得 $pv=1$，从而产生矛盾．由此可知 p 不满足类似定理 3.57 中的欧几里得引理（回忆 $\mathbb{Z}[\mathrm{i}]$ 是 PID），从而根据习题 3.62，p 不是 $\mathbb{Z}[\mathrm{i}]$ 中的不可约元素，因此在 $\mathbb{Z}[\mathrm{i}]$ 中有因式分解

$$p=\alpha\beta,$$

其中 $\alpha=a+\mathrm{i}b$ 和 $\beta=c+\mathrm{i}d$ 都不是单位．因此，取范数得 $\mathbb{Z}$ 中的等式：

$$\begin{aligned}p^2&=\partial(p)\\&=\partial(\alpha\beta)\\&=\partial(\alpha)\partial(\beta)\\&=(a^2+b^2)(c^2+d^2).\end{aligned}$$

由命题 3.64，$\mathbb{Z}[\mathrm{i}]$ 中的单位只有 ±1 和 $\pm\mathrm{i}$，因此任一不是单位的非零高斯整数有 norm >1．于是 $a^2+b^2\neq 1, c^2+d^2\neq 1$．现在欧几里得引理给出 $p\mid(a^2+b^2)$ 或 $p\mid(c^2+d^2)$，算术基本定理给出所要证明的结果 $p=a^2+b^2$（和 $p=c^2+d^2$）. ■

我们要确定 $\mathbb{Z}[\mathrm{i}]$ 中所有不可约元素，但先证明一个引理．

引理 3.67 如果 $\alpha\in\mathbb{Z}[\mathrm{i}]$ 是不可约的，则存在唯一的素数 p 使得在 $\mathbb{Z}[\mathrm{i}]$ 中 $\alpha\mid p$.

证明 注意，如果 $\alpha\in\mathbb{Z}[\mathrm{i}]$，则 $\bar{\alpha}\in\mathbb{Z}[\mathrm{i}]$．因 $\partial(\alpha)=\alpha\bar{\alpha}$，所以有 $\alpha\mid\partial(\alpha)$．现在 $\partial(\alpha)=p_1\cdots p_n$，其中 p_i 是素数．因 $\mathbb{Z}[\mathrm{i}]$ 是 PID，所以由习题 3.62，有某个 i 使得 $\alpha\mid p_i$（因为 α 是不可约的）．如果对某个素数 $q\neq p_i$ 有 $\alpha\mid q$，则 $\alpha\mid(q,p_i)=1$，这迫使 α 必须是单位．这个矛盾表明 p_i 是唯一可以被 α 整除的素数． ■

命题 3.68 设 $\alpha=a+b\mathrm{i}\in\mathbb{Z}[\mathrm{i}]$ 不是 0，也不是单位，则 α 是不可约的当且仅当

（ⅰ）α 是形如 $p=4m+3$ 的素数 p 在 $\mathbb{Z}$ 中的相伴数；或

（ⅱ）α 是 $1+\mathrm{i}$ 或它的共轭 $1-\mathrm{i}$ 的相伴数；或

[155]

㊀ 定理 3.30 说 G 是循环群，因为循环群的每个子群是循环群，所以 S 是循环群，我们这里没有用这个定理，这里给出的证明是更为初等的．

㊁ 费马第一个陈述了该定理，但第一个发表证明的是欧拉．高斯证明只有一对自然数 a，b 满足 $p=a^2+b^2$.

156

(iii) $\partial(\alpha)=a^2+b^2$ 是 Z 中形如 $4m+1$ 的素数．

证明　由引理 3.67，在 Z[i] 中存在唯一的素数 p 被 α 整除．因 $\alpha\mid p$，在Z中有 $\partial(\alpha)\mid\partial(p)=p^2$，从而 $\partial(\alpha)=p$ 或 $\partial(\alpha)=p^2$；即

$$a^2+b^2=p \quad 或 \quad a^2+b^2=p^2.$$

考察 $p$mod4，可以看到有三种可能性（因为 $p\equiv 0$mod4 是不可能的）．

(i) $p\equiv 3$mod4.

此时，由定理 3.66（容易推出的一个方向），不可能有 $a^2+b^2=p$，从而 $\partial(\alpha)=a^2+b^2=p^2$．现在 p 被 α 整除，所以存在 β 使得 $\alpha\beta=p$，因此 $\partial(\alpha)\partial(\beta)=\partial(p)$．因 $p\in$ Z，因而有 $\partial(p)=p^2$，从而 $p^2\partial(\beta)=p^2$，于是 $\partial(\beta)=1$，由命题3.64(i)，β是单位，从而 p 在 Z[i] 中不可约．

(ii) $p\equiv 2$mod4．

此时 $p=2$，从而 $a^2+b^2=2$ 或 $a^2+b^2=4$．后一种情况不可能出现（因为 a 和 b 是整数），第一种情况给出 $\alpha=1\pm\mathrm{i}$，读者需验证 $1+\mathrm{i}$ 和 $1-\mathrm{i}$ 事实上都是不可约元素．

(iii) $p\equiv 1$mod4.

如果 $\partial(\alpha)$ 是一个素数 p（满足 $p\equiv 1$mod4），则由命题 3.64（ii），α 是不可约的．反之，假定 α 是不可约的．因 $\partial(\alpha)=p$ 或 $\partial(\alpha)=p^2$，所以只需排除后一种情形．因 $\alpha\mid p$，对某个 $\beta\in$ Z[i] 有 $p=\alpha\beta$．因此和情形（i）一样，$\partial(\alpha)=p^2$ 蕴涵 β是单位．现在 $\alpha\overline{\alpha}=p^2=(\alpha\beta)^2$，从而 $\overline{\alpha}=\alpha\beta^2$，但由命题3.64(iii)，$\beta^2=\pm 1$，这与 $\overline{\alpha}\neq\pm\alpha$ 矛盾．所以 $\partial(\alpha)=p$．■

例如，3 是第一类型的不可约元素，$2+\mathrm{i}$ 是第三类型的不可约元素．我们应该记住在素数和不可约高斯整数之间有着有趣的联系，应该知道高斯单位是十分有价值的概念，以及范数在证明中是一个有用的工具．高斯整数环是代数整数环的一个例子，以上注释对于代数整数环也成立．

习题

定义：设 k 是域．$k[x]$ 中 $a_1(x),a_2(x),\cdots,a_n(x)$ 的**公因式**是指多项式 $c(x)\in k[x]$，对一切 i 满足 $c(x)\mid a_i(x)$．**最大公因式**是指次数最高的首一公因式，记为 $c(x)=(a_1,a_2,\cdots,a_n)$.

3.57　设 k 是域，并设 $a_1(x),a_2(x),\cdots,a_n(x)$ 是 $k[x]$ 中给定的多项式．

(i) 证明这些多项式的最大公因式 $d(x)$ 形如 $\sum t_i(x)a_i(x)$，其中对 $1\leqslant i\leqslant n, t_i(x)\in k[x]$．

提示：例 3.49.

157

(ii) 证明对 $a_i(x)$ 的每个首一公因式 $c(x)$ 有 $c(x)\mid d(x)$．

3.58　(i) 证明 $x,y\in k[x,y]$ 互素，但 1 不是它们的线性组合［即不存在 $s(x,y),t(x,y)\in k[x,y]$ 使得 $1=xs(x,y)+yt(x,y)$］．

提示：用次数推导．

(ii) 证明 2 和 x 在 Z$[x]$ 中互素，但 1 不是它们的线性组合；即不存在 $s(x),t(x)\in$ Z$[x]$ 使得 $1=2s(x)+xt(x)$．

3.59　一个学生宣称 $x-1$ 不是不可约的，因为 $x-1=(\sqrt{x}+1)(\sqrt{x}-1)$ 是一个因式分解．说明他的方法错在哪里．

提示：证明$\sqrt{x}+1$不是多项式．

3.60　证明存在这样的整环，它包含一对没有 gcd 的元素．（见 147 页的定义．）

提示：设 k 是域，并设 R 是$k[x]$中由一切没有线性项的多项式组成的子环，即 $f(x)\in R$ 当且仅当

$$f(x) = s_0 + s_2x^2 + s_3x^3 + \cdots.$$

证明 x^5 和 x^6 在 R 中没有 gcd.

3.61 证明 $R = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a,b \in \mathbb{Z}\}$ 是带有 $\partial(a + b\sqrt{2}) = |a^2 - 2b^2|$ 的欧几里得环.

3.62 如果 R 是欧几里得环且 $\pi \in R$ 不可约，证明 $\pi \mid \alpha\beta$ 蕴涵 $\pi \mid \alpha$ 或 $\pi \mid \beta$.

3.63 设 ∂ 是欧几里得环 R 的次数函数. 如果 $m,n \in \mathbb{N}$ 且 $m \geqslant 1$，证明 ∂' 也是 R 上的次数函数，其中对一切 $x \in R$，

$$\partial'(x) = m\partial(x) + n.$$

由此可知，一个欧几里得环可以没有次数为 0 或次数为 1 的元素.

3.64 设 R 是带有次数函数 ∂ 的欧几里得环.

(i) 证明对一切非零 $a \in R$, $\partial(1) \leqslant \partial(a)$.

(ii) 证明非零 $u \in R$ 是单位当且仅当 $\partial(u) = \partial(1)$.

提示：把多项式这种特殊情形的证明加以推广.

3.65 设 R 是欧几里得环，并假定 $b \in R$ 不是零也不是单位. 证明对每个 $i \geqslant 0$，$\partial(b^i) < \partial(b^{i+1})$.

提示：存在 $q,r \in R$ 使得 $b^i = qb^{i+1} + r$.

3.66 如果 p 是素数且 $p \equiv 3 \bmod 4$，证明同余式 $a^2 \equiv 2 \bmod p$ 或 $a^2 \equiv -2 \bmod p$ 有解.

提示：证明 $\mathbb{I}_p^\times \cong \langle -1 \rangle \times H$，其中 H 是阶为奇数 m 的群，比如 $\mathbb{I}_m$，因为

$$\mathbb{I}_2 \times \mathbb{I}_m = (\{1\} \times H) \cup (\{-1\} \times H),$$

所以 2 或 −2 在 H 中. 最后用习题 2.54.

3.7 线性代数

暂且中断环论的讲解转而讨论线性代数，它是进一步研究交换环的必要工具. [158]

3.7.1 向量空间

线性代数研究向量空间及其同态以及它在线性方程组中的应用. 从现在起，假定大多数读者已经学过有关矩阵的一些课程，也许其元素只限于实的或复的. 这些课程往往注重于计算，如高斯消元法、求逆、行列式、特征向量和矩阵的特征多项式，线性代数的这些内容固然重要，但不是本书的重点，本书将讨论向量空间（标量在任意域上）更理论化的性质以及线性变换（向量空间之间的同态）.

维数是一个十分微妙的概念. 平面上的一条曲线是一个连续函数 $f : \mathbb{R} \to \mathbb{R}^2$ 的象，它是二维环绕空间中的一维子集. 19 世纪末当一条"充满空间的曲线"被发现的时候，混乱可以想见：竟存在一个连续函数 $f : \mathbb{R} \to \mathbb{R}^2$ 其象充满平面！我们将在类似于欧几里得空间的向量空间中，描述定义维数的一种方法（有定义更一般空间维数的拓扑方法）.

定义 *设 k 是域，则 k 上的向量空间是一个配置了标量乘法的（加法）阿贝尔群 V，就是说，有一个函数 $k \times V \to V$，记为 $(a,v) \mapsto av$，它使得对一切 $a,b,1 \in k$ 和 $u,v \in V$，有*

(i) $a(u + v) = au + av$;

(ii) $(a + b)u = av + bv$;

(iii) $(ab)v = a(bv)$;

(iv) $1v = v$.

称 V 的元素为**向量**，k 的元素为**标量**[⊖].

例 3.69　（ⅰ）欧几里得空间 $v=\mathbb{R}^n$ 是$\mathbb{R}$上的向量空间，向量是 n 元组 $(a_1,\cdots,a_n)$，其中对一切 $i,a_i\in\mathbb{R}$. 可以把向量 v 画成从原点到坐标为 $(a_1,\cdots a_n)$ 的点的箭头. 加法由

$$(a_1,\cdots,a_n)+(b_1,\cdots,b_n)=(a_1+b_1,\cdots,a_n+b_n)$$

给出，几何上两向量的和由平行四边形法则描述.

标量乘法由

$$av=a(a_1,\cdots,a_n)=(aa_1,\cdots,aa_n)$$

159 给出.

标量乘法 $v\mapsto av$ 是把 v "伸长" $|a|$ 倍，当 a 为负时，则改变为反方向（伸长加引号是因为当 $|a|<1$ 时，av 比 v 短）.

（ⅱ）（ⅰ）中的例子可以推广. 如果 k 是任一域，则定义 $V=k^n$，即一切 n 元组 $v=(a_1,\cdots,a_n)$ 的集合，其中对一切 $i,a_i\in k$. 加法由

$$(a_1,\cdots,a_n)+(b_1,\cdots,b_n)=(a_1+b_1,\cdots,a_n+b_n)$$

给出，标量乘法由

$$av=a(a_1,\cdots,a_n)=(aa_1,\cdots,aa_n)$$

给出.

（ⅲ）如果 R 是交换环而 k 是构成域的子环，则 R 是 k 上的向量空间. 把 R 的元素看作向量，把 k 的元素看作标量，则对 $a\in k$ 和 $v\in R$ 定义标量乘法 av 为该两个元素在 R 中的积. 注意向量空间定义中的公理只是交换环中成立的部分公理的特殊情形.

例如，如果 k 是域，则多项式环 $R=k[x]$ 是 k 上的向量空间. 向量是多项式 $f(x)$，标量是元素 $a\in k$，标量乘法给出多项式 $af(x)$；即如果

$$f(x)=b_nx^n+\cdots+b_1x+b_0,$$

则

$$af(x)=ab_nx^n+\cdots+ab_1x+ab_0.$$

特别地，如果域 k 是一个更大域 E 的子域，则 E 是 k 上的向量空间. ■

向量空间 V 的子空间是指 V 的一个子集，它在 V 中的加法和标量乘法下构成向量空间.

定义　如果 V 是域 k 上的向量空间，则 V 的**子空间**是 V 的子集 U 满足

（ⅰ）$0\in U$；

（ⅱ）$u,u'\in U$ 蕴涵 $u+u'\in U$；

（ⅲ）$u\in U$ 和 $a\in k$ 蕴涵 $au\in U$.

例 3.70　（ⅰ）极端情形 $U=V$ 和 $U=\{0\}$（其中 $\{0\}$ 表示只由零向量组成的子集）恒为向量空

160 间的子空间. 称子空间 $U\subseteq V$ 且 $U\neq V$ 为 V 的**真子空间**，可以用 $U\subsetneq V$ 来记 U 是 V 的真子空间.

（ⅱ）如果 $v=(a_1,\cdots,a_n)$ 是 $\mathbb{R}^n$ 中的非零向量，则过原点的直线

$$\ell=\{av:a\in\mathbb{R}\}$$

是$\mathbb{R}^n$ 的子空间.

类似地，过原点的平面由形如 av_1+bv_2 的一切向量所构成，其中 v_1,v_2 是一对不共线的固定向

⊖ vector（向量）一词来自意为"携带"的拉丁词，在欧几里得空间，vector 携带了长度和方向的数据. Scalar（标量）一词是出于把 $v\mapsto av$ 看作尺度的改变，scale 和 scalar 都来自意为"梯子"的拉丁词，因为梯子的横档是均匀排列的.

量，并且 a,b 遍历$\mathbb{R}$．容易验证这种过原点的平面是 $\mathbb{R}^n$ 的子空间．

（ⅲ）如果 $m \leqslant n$ 且把 $\mathbb{R}^m$ 看作$\mathbb{R}^n$ 中所有最后 $n-m$ 个坐标都是 0 的向量的集合，则 $\mathbb{R}^m$ 是 $\mathbb{R}^n$ 的子空间．例如，可以把平面$\mathbb{R}^2$ 看作$\mathbb{R}^3$ 中的一切点（x，y，0）．

（ⅳ）如果 k 是域，则 k 上 n 个未知量、m 个方程的**齐次线性方程组**是方程组

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= 0 \\ a_{21}x_1 + \cdots + a_{2n}x_n &= 0 \\ &\vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n &= 0, \end{aligned}$$

其中 $a_{ji} \in k$．该方程组的**解**是向量 $(c_1,\cdots,c_n) \in k^n$，其中对一切 j，$\sum_i a_{ji}c_i = 0$；如果有某个 $c_i \neq 0$，则称解 $(c_1,\cdots,c_n)$ 是**非平凡的**．一切解的集合形成 k^n 的子空间，称为该方程组的**解空间**（或零空间）．

特别地，可以解 $\mathbb{I}_p$ 上的线性方程组，其中 p 是素数．也就是说可以像对待常规方程组那样对待 mod$p$ 的同余方程组．

例如，同余方程组

$$\begin{aligned} 3x - 2y + z &\equiv 1 \bmod 7 \\ x + y - 2z &\equiv 0 \bmod 7 \\ -x + 2y + z &\equiv 4 \bmod 7 \end{aligned}$$

可以看作域 $\mathbb{I}_7$ 上的方程组．中学就能够解出该方程组，因为 mod7 的逆是：$[2][4]=[1]$；$[3][5]=[1]$；$[6][6]=[1]$．解为

$$(x,y,z) = ([5],[4],[1]).$$ ■

定义 称向量空间 V 中的一组有序向量的集合 $v_1,\cdots,v_n$ 为 V 中的一张**表**．

更准确地说，对于 $n \geqslant 1$，有函数

$$\varphi:\{1,2,\cdots,n\} \to V,$$

其中对一切 i，$\varphi(i) = v_i$．于是，$X = \mathrm{im}\varphi$．注意 X 在下面的意义下是有序的：第一个向量为 v_1，第二个向量为 v_2，等等．一个向量可以在表中出现数次，即 φ 不必是单射．

[161]

定义 设 V 是域 k 上的向量空间，V 中表 $v_1,\cdots,v_n$ 的一个 **k－线性组合**是形如

$$v = a_1v_1 + \cdots + a_nv_n$$

的向量 v，其中对一切 i，$a_i \in k$．

定义 如果 $X = v_1,\cdots,v_m$ 是向量空间 V 中的表，则 $v_1,\cdots,v_m$ 的一切 k－线性组合构成的集合

$$\langle v_1,\cdots,v_m\rangle$$

称为 **X 张成的子空间**，也称 $v_1,\cdots,v_m$ **张成** $\langle v_1,\cdots,v_m\rangle$．

引理 3.71 设 V 是域 k 上的向量空间．

（ⅰ）V 的子空间的交是子空间．

（ⅱ）如果 $X = v_1,\cdots,v_m$ 是 V 中的表，则 V 的包含 X 的一切子空间的交是 $v_1,\cdots,v_m$ 张成的子空间 $\langle v_1,\cdots v_m\rangle$，因此 $\langle v_1,\cdots,v_m\rangle$ 是 V 的包含 X 的**最小**子空间．

证明概要 （ⅰ）的结论是自然的．设 $X = \{v_1,\cdots,v_m\}$，记$\mathcal{S}$为 V 的包含 X 的一切子空间的族，则

$$\bigcap_{S\in\mathcal{S}} S = \langle v_1,\cdots,v_m\rangle.$$

因为 $\langle v_1,\cdots,v_m\rangle \in \mathcal{S}$，所以包含关系$\subseteq$是显然的．关于反包含，注意到如果 $S\in\mathcal{S}$，则 S 包含 $v_1,\cdots,v_m$，因此它包含 $v_1\cdots,v_m$ 的一切线性组合的集合，即 $\langle v_1,\cdots,v_m\rangle$. ■

由引理的第二部分可知，表 $X = v_1,\cdots,v_m$ 张成的子空间并不依赖于向量的序，而只依赖于向量集本身．为使代数术语一致起见，可称 $\langle v_1,\cdots,v_m\rangle$ 为 X 生成的子空间，之所以产生不同的术语是因为群论、环论和向量空间的理论都是各自独立发展起来的．

如果 $X=\varnothing$，则 $\langle X\rangle=\bigcap_{S\in\mathcal{S}}S$，其中$\mathcal{S}$是 V 的包含 X 的一切子空间的族．因为每个子空间都包含 $X=\varnothing$，而 $\{0\}$ 本身也是子空间，也出现在 V 的一切子空间的交之中，由此，$\langle\varnothing\rangle=\bigcap_{S\subseteq V}S=\{0\}$．

例 3.72 （ⅰ）设 $V=\mathbb{R}^2, e_1=(1,0), e_2=(0,1)$. 现在 $V=\langle e_1,e_2\rangle$，这是因为如果 $v=(a,b)\in V$，则

162

$$\begin{aligned} v &= (a,0)+(0,b) \\ &= a(1,0)+b(0,1) \\ &= ae_1+be_2 \in \langle e_1,e_2\rangle. \end{aligned}$$

（ⅱ）如果 k 是域且 $V=k^n$，定义 e_i 为第 i 个坐标为 1，其余为 0 的 n 元组．读者只需对（ⅰ）的论证略加修改，即可证明 $e_1,\cdots,e_n$ 张成 k^n.

（ⅲ）向量空间 V 并不一定由有限表所张成．例如，$V=k[x]$，并假定 $X=f_1(x),\cdots,f_m(x)$ 是 V 中的有限表．令 d 是一切 $f_i(x)$ 的最高次数，则 $f_1(x),\cdots,f_m(x)$ 的每个（非零）k-线性组合的次数最多是 d. 由此，x^{k+1} 不是 X 中向量的 k-线性组合，从而 X 不能张成 $k[x]$. ■

即使还没有定义维数，下面的定义仍是有意义的．

定义 由有限表张成的向量空间 V 称为是**有限维的**，否则称 V 为**无限维的**．

例3.72（ⅱ）表明 k^n 是有限维的，而该例的第（ⅲ）部分表明 $k[x]$ 是无限维的．由例 3.69（ⅲ），$\mathbb{R}$ 和$\mathbb{C}$ 都是$\mathbb{Q}$ 上的向量空间，它们都是无限维的．

记号 如果 $v_1,\cdots,v_m$ 是表，则记 $v_1,\cdots,\hat{v}_i,\cdots,v_m$ 为删除 v_i 后缩短的表．

命题 3.73 如果 V 是向量空间，则对于张成 V 的表 $X=v_1,\cdots,v_m$，下列条件等价：

（ⅰ）X 不是最短的张成表；

（ⅱ）有某个 v_i 在其他向量张成的子空间中；即

$$v_i \in \langle v_1,\cdots,\hat{v}_i,\cdots,v_m\rangle;$$

（ⅲ）存在不全为零的标量 $a_1,\cdots,a_m$ 使得

$$\sum_{\ell=1}^{m} a_\ell v_\ell = 0.$$

证明概要 （ⅰ）⇒（ⅱ）．如果 X 不是最短张成 V 的表，则可在 X 中剔除一个向量，而缩短的表仍张成 X.

（ⅱ）⇒（ⅲ）．如果 $v_i=\sum_{j\neq i}c_jv_j$，则定义 $a_i=-1\neq 0$ 且对一切 $j\neq i$，令 $a_j=c_j$．

（ⅲ）⇒（ⅰ）．给出的等式蕴涵向量之一（比如 v_i）是其他向量的线性组合．于是，删除 v_i 后缩短的表仍然张成 X：如果 $v\in V$ 是所有 v_j（包括 v_i）的线性组合，只要在表达式中把 v_i 替换为其他 v_j 的线性组合然后合并同类项即可． ■

163

定义 称向量空间中的表 $X = v_1, \cdots, v_m$ **线性相关**，如果存在不全为零的标量 $a_1, \cdots, a_m$ 使得 $\sum_{\ell=1}^{m} a_\ell v_\ell = 0$；否则称 X **线性无关**.

空集 $\varnothing$ 定义为线性无关（可以把它当作长度为 0 的表）.

例 3.74 （i）包含零向量的任一表 $X = v_1, \cdots, v_m$ 线性相关.

（ii）长度为 1 的表 v_1 线性相关当且仅当 $v_1 = 0$；因此，长度为 1 的表 v_1 线性无关当且仅当 $v_1 \neq 0$.

（iii）表 v_1, v_2 线性相关当且仅当其中一个向量是另一的标量倍.

（iv）如果表 $v_1, \cdots, v_m$ 中有重复（即对某个 $i \neq j$ 有 $v_i = v_j$），则 $v_1, \cdots, v_m$ 线性相关：定义 $c_i = 1, c_j = -1$，其他一切 $c = 0$. 所以，如果 $v_1, \cdots, v_m$ 线性无关，则所有向量 v_i 都是不同的. ■

命题 3.73 的对应命题值得一提.

系 3.75 如果 $X = v_1, \cdots, v_m$ 是张成向量空间 V 的表，则 X 是张成 V 的最短的表当且仅当 X 线性无关.

和线性相关不同，线性无关是间接定义的. 由于线性无关的重要性，再给出其直接定义. 称表 $X = v_1, \cdots, v_m$ **线性无关**，如果 k-线性组合 $\sum_{\ell=1}^{m} a_\ell v_\ell = 0$ 蕴涵每个 $a_i = 0$. 由此，线性无关表的每个子表线性无关（这是规定 $\varnothing$ 是线性无关的一个理由）.

现在要讨论一直探索的概念.

定义 向量空间 V 的**基**是指张成 V 的线性无关表.

由此，基是张成向量空间的最短表. 由例3.74(iv)，线性无关表 $v_1, \cdots, v_m$ 中的所有向量当然是各不相同的.

例 3.76 在例3.72(ii)中可以看到 $X = e_1, \cdots, e_n$ 张成 k^n，其中 e_i 是第 i 个坐标为 1，其他为 0 的 n 元组. 容易证明 X 线性无关因而是基，这个基称为 k^n 的**标准基**. ■

命题 3.77 设 $X = v_1, \cdots, v_n$ 是域 k 上的向量空间 V 中的表，则 X 是基当且仅当 V 中的每个向量都能唯一地表示为 X 中向量的 k-线性组合.

164

证明概要 如果向量 $v = \sum a_i v_i = \sum b_i v_i$，则 $\sum (a_i - b_i) v_i = 0$. 由无关性，对一切 i 有 $a_i = b_i$，即表示法唯一.

反之，表示法的存在性说明表 X 张成 V. 此外，如果 $0 = \sum c_i v_i$，且非一切 $c_i = 0$，则向量 0 表示为 v_i 的线性组合不唯一. ■

定义 如果 $X = v_1, \cdots, v_n$ 是向量空间 V 的基，$v \in V$，则存在唯一的标量 $a_1, \cdots, a_n$ 使得 $v = \sum_{i=1}^{n} a_i v_i$. 称 n 元组 $(a_1, \cdots, a_n)$ 为向量 $v \in V$ 关于基 X 的**坐标集**.

如果 $v_1, \cdots, v_n$ 是 $V = k^n$ 的标准基，则关于这个基的坐标集就是通常的坐标集.

如果 $v_1, \cdots, v_n$ 是域 k 上的向量空间 V 的基，则每个向量 $v \in V$ 都有唯一的表达式

$$v = a_1 v_1 + a_2 v_2 + \cdots + a_n v_n,$$

其中对一切 i, $a_i \in k$. 因为有第一个向量 v_1，第二个向量 v_2，等等，所以 k-线性组合中的系数唯一地确定了一个 n 元组 $(a_1, a_2, \cdots, a_n)$. 要是基仅仅是 V 的子集而不是表（即有序子集），则每个向量会有 $n!$ 个坐标集.

下面准备定义向量空间 V 的维数为基中向量的个数，这时立即带来两个问题.

（ⅰ）每个向量空间是否都有基？

（ⅱ）向量空间的每个基的元素个数是否都相同？

第一个问题容易回答，而第二个问题需要一点思考．

定理 3.78 每个有限维向量空间 V 都有基．

证明概要 因 V 是有限维的，存在张成 V 的有限表 X. 如果 X 线性无关，它就是一个基；否则，由命题 3.73，X 可以缩短为张成 V 的子表 X'．如果 X' 线性无关，它就是基；否则，X' 又可以缩短为张成 V 的子表 X''．最终得到张成 V 的最短子表，它必线性无关，因此它是基． ■

张成和线性无关的定义可以扩张到向量空间中的无限表上，从而可以证明无限维向量空间也有基（见定理 6.48）．例如，可以导出 $k[x]$ 上的基是 $1,x,x^2,\cdots,x^n,\cdots$.

现证明维数的不变性，它是向量空间最重要的结果之一．

引理 3.79 设 $u_1,\cdots u_n$ 是向量空间 V 的元素，并设 $v_1,\cdots,v_m \in \langle u_1,\cdots,u_n\rangle$．如果 $m>n$，则 $v_1,\cdots,v_m$ 是线性相关表．

165

证明 对 $n\geqslant 1$ 用归纳法证明．

基础步．如果 $n=1$，则至少有两个向量 v_1,v_2 满足 $v_1=a_1u_1,v_2=a_2u_1$．如果 $u_1=0$，则 $v_1=0$，从而诸 v 组成的表线性相关．假设 $u_1\neq 0$，可以假定 $v_1\neq 0$，否则结论已经成立，由此 $a_1\neq 0$．因此由 $v_2-a_2a_1^{-1}v_1=0$ 可知 v_1 和 v_2 线性相关，因此大表 $v_1,\cdots,v_m$ 线性相关．

归纳步．对 $i=1,\cdots,m$，有等式

$$v_i=a_{i1}u_1+\cdots+a_{in}u_n.$$

可假定某个 $a_{i1}\neq 0$，否则 $v_1,\cdots,v_m\in\langle u_2,\cdots,u_n\rangle$，由归纳假设可得结论．如有必要改变记号（即对诸 v 重新排序），可假定 $a_{11}\neq 0$．对每个 $i\geqslant 2$，定义

$$v_i'=v_i-a_{i1}a_{11}^{-1}v_1\in\langle u_2,\cdots,u_n\rangle$$

（把 v_i' 表示为诸 u 的线性组合后，u_1 的系数是 $a_{i1}-(a_{i1}a_{11}^{-1})a_{11}=0$）．因 $m-1>n-1$，由归纳假设存在不全为 0 的标量 $b_2,\cdots,b_m$ 使得

$$b_2v_2'+\cdots+b_mv_m'=0.$$

用 v_i' 的定义重写上面的等式：

$$\Big(-\sum_{i\geqslant 2}b_ia_{i1}a_{11}^{-1}\Big)v_1+b_2v_2+\cdots+b_mv_m=0.$$

其中系数不全为 0，因此 $v_1,\cdots,v_m$ 线性相关． ■

下面熟知的事实说明线性代数和线性方程组之间的密切关系．

系 3.80 域 k 上的一个齐次线性方程组，如果其未知数的个数多于方程的个数，则必有非平凡解．

证明 n 元组 $(\beta_1,\cdots,\beta_n)$ 是方程组

$$\begin{aligned}\alpha_{11}x_1+\cdots+\alpha_{1n}x_n&=0\\ &\vdots\\ \alpha_{m1}x_1+\cdots+\alpha_{mn}x_n&=0\end{aligned}$$

的解，如果对一切 i，$\alpha_{i1}\beta_1+\cdots+\alpha_{in}\beta_n=0$. 换句话说，如果 $m\times n$ 系数矩阵 $A=[\alpha_{ij}]$ 的列为 $c_1,\cdots,c_n$，则

$$\beta_1c_1+\cdots+\beta_nc_n=0.$$

注意 $c_i\in k^m$，现在 k^m 可由 m 个向量张成（例如标准基）．因为由假设，$m>n$，据引理 3.79，表

$c_1,\cdots,c_n$ 线性相关．于是存在不全为零的标量 $\gamma_1,\cdots,\gamma_n$ 使得 $\gamma_1 c_1+\cdots+\gamma_n c_n=0$，因此 $(\gamma_1,\cdots,\gamma_n)$ 是方程组的一个非平凡解． ■ [166]

定理 3.81（维数的不变性） 如果 $X=x_1,\cdots,x_n$ 和 $Y=y_1,\cdots,y_m$ 都是向量空间 V 的基，则 $m=n$．

证明 如果 $m\neq n$，则要么 $n<m$ 要么 $m<n$．在第一种情形中，因 X 张成 V，所以 $y_1,\cdots,y_m\in\langle x_1,\cdots,x_n\rangle$，根据引理 3.79，$Y$ 线性相关，于是产生矛盾．如果 $m<n$，同样引出矛盾．因此必有 $m=n$． ■

现在可作下列定义．

定义 如果 V 是域 k 上的有限维向量空间，则它的**维数**是 V 的基中所含元素的个数，记为 $\dim_k(V)$ 或 $\dim(V)$．

例 3.82 （i）例 3.76 表明 k^n 是 n 维的，当 $k=\mathbb{R}$ 时，这与我们的直觉一致．于是，平面 $\mathbb{R}\times\mathbb{R}$ 是二维的！

（ii）如果 $V=\{0\}$，则由于没有元素在它的基 $\varnothing$ 之中，因此 $\dim(V)=0$．（这是定义 $\varnothing$ 线性无关的好理由．）

（iii）设 $X=\{x_1,\cdots,x_n\}$ 是有限集．定义

$$k^X=\{\text{函数 } f: X\to k\}.$$

如果定义加法 $f+f'$ 为

$$f+f': x\mapsto f(x)+f'(x),$$

并对 $a\in k$ 和 $f: X\to k$ 定义标量乘法为

$$af: x\mapsto af(x),$$

则 k^X 是一个向量空间．对 $x\in X$，定义

$$f_x(y)=\begin{cases}1 & \text{当 } y=x;\\ 0 & \text{当 } y\neq x,\end{cases}$$

容易验证 n 个形如 f_x 的函数组成一个基，从而 $\dim(k^X)=n=|X|$．

读者应注意到这并不是一个新的例子．其实一个 n 元组 $(a_1,\cdots,a_n)$ 就是函数 $f:\{1,\cdots,n\}\to k$，其中对一切 i 有 $f(i)=a_i$．于是，函数 f_x 组成标准基． ■

下面是维数不变性的第二个证明，在第 6 章中要用它来推广维数的概念到超越次数的概念．现从修改命题 3.73 的证明开始．

引理 3.83 如果 $X=v_1,\cdots,v_n$ 是向量空间 V 中线性相关的向量表，则存在 v_r（其中 $r\geqslant 1$）满足 $v_r\in\langle v_1,\cdots,v_{r-1}\rangle$［当 $r=1$ 时，把 $\langle v_1,\cdots,v_{r-1}\rangle$ 看作 $\{0\}$］． [167]

注 把命题 3.73 和这个命题作一比较．先前的命题说，如果 v_1,v_2,v_3 线性相关，则或者 $v_1\in\langle v_2,v_3\rangle$，或者 $v_2\in\langle v_1,v_3\rangle$，或者 $v_3\in\langle v_1,v_2\rangle$．这个命题说，或者 $v_1\in\{0\}$，或者 $v_2\in\langle v_1\rangle$，或者 $v_3\in\langle v_1,v_2\rangle$．

证明 设 r 是使得 $v_1,\cdots,v_{r-1}$ 线性无关的最大整数．如果 $v_1=0$，则 $v_1\in\{0\}$，于是结论成立．如果 $v_1\neq 0$，则 $r\geqslant 2$．由 $v_1,\cdots,v_n$ 线性相关知 $r-1<n$. 因 $r-1$ 是最大的，所以表 $v_1,v_2,\cdots,v_r$ 线性相关，从而存在不全为零的标量 $a_1,\cdots a_r$ 使得 $a_1v_1+\cdots+a_rv_r=0$．在这个表达式中必有 $a_r\neq 0$，否则 $v_1,\cdots,v_{r-1}$ 将线性相关．因此

$$v_r=\sum_{i=1}^{r-1}(-a_r^{-1})a_iv_i\in\langle v_1,\cdots,v_{r-1}\rangle.$$ ■

引理 3.84（替换引理） 设 $X = x_1, \cdots, x_m$ 是向量空间 V 的基，$y_1, \cdots, y_n$ 是 V 的线性无关的子集，则 $n \leqslant m$.

证明 先证明 y_n 可替换 X 中诸 x 之一从而新表仍然张成 V. 因 X 张成 V，所以 $y_n \in \langle X \rangle$，从而由命题 3.73，

$$y_n, x_1, \cdots, x_m$$

线性相关. 因为表 $y_1, \cdots, y_n$ 线性无关，所以 $y_n \notin \{0\}$. 根据引理 3.83，存在某个 i 使得 $x_i = a y_n + \sum_{j<i} a_j x_j$. 在基 $x_1, \cdots, x_m$ 中删除 x_i 代之以 y_n 得到表

$$X' = y_n, x_1, \cdots, \hat{x}_i, \cdots, x_m:$$

它仍然张成 V，这是因为如果 $v = \sum_{j=1}^{m} b_j x_j$，则（如同命题 3.73 的证明那样）替换 x_i 为其他诸 x 和 y_n 的 k-线性组合，再合并同类项.

对张成 V 的表 $y_{n-1}, y_n, x_1, \cdots, \hat{x}_i \cdots, x_m$ 重复以上论证. 对于该线性相关表，引理 3.83 所提供的选择是 $y_n \in \langle y_{n-1} \rangle, x_1 \in \langle y_{n-1}, y_n \rangle, x_2 \in \langle y_{n-1}, y_n, x_1 \rangle$，等等. 因 Y 线性无关，所以其子表 y_{n-1}, y_n 也线性无关，从而第一项 $y_n \in \langle y_{n-1} \rangle$ 是不可能的. 于是（引理 3.83 保证）必可选择剩余的向量即诸 x 中的一个，比如 x_ℓ. 删除 x_ℓ 可得新的张成 V 的表 X''. 如此重复构造张成 V 的表，因 $y_i \in \langle y_{i+1}, \cdots, y_n \rangle$ 是不可能的，所以每一次一个新的 y 添加为第一个向量，而删除一个 x. 如果 $n > m$，即 y 的个数比 x 的个数多，则该过程最后得到由 m 个 y 组成的张成 V 的表（m 个 x 被一个一个删除），其中没有 x. 于是 $Y = y_1, \cdots, y_n$ 的一个真子表张成 V，而这与 Y 线性无关矛盾，所以 $n \leqslant m$. ■

168

定理 3.85（维数的不变性） 如果 $X = x_1, \cdots, x_m$ 和 $Y = y_1, \cdots, y_n$ 都是向量空间 V 的基，则 $m = n$. ■

证明 根据引理 3.84，把有 m 个元素的 X 看作基，而把有 n 个元素的 Y 看作线性无关表给出不等式 $n \leqslant m$；把 Y 看作基而把 X 看作线性无关表又给出相反的不等式 $m \leqslant n$，所以 $m = n$. ■

定义 **最长（或极大）**线性无关表 $u_1, \cdots, u_m$ 是指这样一个线性无关表，对于它没有向量 $v \in V$ 可以使得 $u_1, \cdots, u_m, v$ 线性无关.

引理 3.86 如果 V 是有限维向量空间，则最长线性无关表 $v_1, \cdots, v_n$ 是 V 的基.

证明概要 如果该表不是基，则它不能张成 V，即有 $w \in V$ 满足 $w \notin \langle v_1, \cdots, v_n \rangle$. 但根据命题 3.73，添加 w 后形成的加长表线性无关. ■

最长线性无关表的存在性并不是显而易见的，下面的结果导出它的存在性，而该结果本身也十分有用.

命题 3.87 设 $Z = u_1, \cdots, u_m$ 是 n 维向量空间 V 中的线性无关表，则 Z 可扩展成 V 的基，即存在向量 $v_{m+1}, \cdots, v_n$ 使得 $u_1, \cdots, u_m, v_{m+1}, \cdots, v_n$ 是 V 的基.

证明概要 如果线性无关表 Z 不张成 V，则有 $w_1 \in V$ 满足 $w_1 \notin \langle Z \rangle$，由命题 3.73，加长表 Z, w_1 线性无关. 如果 Z, w_1 不张成 V，则有 $w_2 \in V$ 满足 $w_2 \notin \langle Z, w_1 \rangle$. 因 $\dim(V) = n$，这种加长表的长度不能够超过 n，否则用替换引理，即引理 3.84，把含有 $n+1$ 个元素的线性无关表和一个基相比较将产生矛盾. ■

系 3.88 如果 $\dim(V) = n$，则 $n+1$ 个或多于 $n+1$ 个向量构成的表线性相关.

证明概要 否则的话，这样的表能够扩张成一个有过多元素的基. ■

系 3.89 设 V 是向量空间满足 $\dim(V)=n$.

（i）张成 V 的 n 个向量的表必线性无关.

（ii）任一含有 n 个向量的线性无关表必张成 V.

169

证明概要 （i）如线性相关，则该表可缩短而成为基，但该基太小.

（ii）如果该表不能张成 V，则它可以加长而成为基，但该基太大. ■

系 3.90 设 U 是 n 维向量空间 V 的子空间.

（i）U 是有限维的且 $\dim(U)\leqslant\dim(V)$.

（ii）如果 $\dim(U)=\dim(V)$，则 $U=V$.

证明概要 （i）取 $u_1\in U$. 如果 $U=\langle u_1\rangle$，则 U 是有限维的，否则就有 $u_2\notin\langle u_1\rangle$. 由命题 3.73，$u_1,u_2$ 线性无关. 如果 $U=\langle u_1,u_2\rangle$，则结论成立. 这个过程不可能重复 $n+1$ 次，否则 $u_1,\cdots,u_{n+1}$ 将构成 $U\subseteq V$ 中的线性无关表，与系 3.88 矛盾.

U 的基是线性无关的，因此它可以扩张为 V 的基.

（ii）如果 $\dim(U)=\dim(V)$，则 U 的基就已经是 V 的基（否则，它可以扩张为 V 的基，而作为 V 的基太大）. ■

习题

3.67 如果向量空间 V 只有子空间 $\{0\}$ 和 V 自身，证明 $\dim(V)\leqslant 1$.

3.68 证明在定义向量空间时，列出所有其他公理后，向量加法的交换律是多余的；即如果 V 满足所有其他公理，则对一切 $u,v\in V,u+v=v+u$.

提示：如果 $u,v\in V$，用两种方法计算 $-[(-v)+(-u)]$.

3.69 如果 V 是 $\mathbb{I}_2$ 上的向量空间，$v_1\neq v_2$ 是 V 中的非零向量，证明 v_1,v_2 线性无关. 在任意其他域上的向量空间这个结果也成立吗?

3.70 证明域 k 上 $m\times n$ 矩阵 A 的列向量在 k^m 中线性相关当且仅当齐次方程组 $Ax=0$ 有非平凡解.

3.71 如果 U 是域 k 上向量空间 V 的子空间，定义商群 V/U 上的标量乘法为

$$\alpha(v+U)=\alpha v+U,$$

其中 $\alpha\in k,v\in V$. 证明这是一个合理定义的函数，它把 V/U 变成 k 上的一个向量空间（称 V/U 为**商空间**）.

3.72 如果 V 是有限维向量空间，U 是子空间，证明

$$\dim(U)+\dim(V/U)=\dim(V).$$

提示：证明如果 $v_1+U,\cdots,v_r+U$ 是 V/U 的基，则表 $v_1,\cdots,v_r$ 线性无关.

170

定义：如果 U 和 W 是向量空间 V 的子空间，定义

$$U+W=\{u+w:u\in U,w\in W\}.$$

3.73 （i）证明 $U+W$ 是 V 的子空间.

（ii）如果 U 和 U' 是有限维向量空间 V 的子空间，证明

$$\dim(U)+\dim(U')=\dim(U\cap U')+\dim(U+U').$$

提示：取 $U\cap U'$ 的基，并把它扩张为 U 和 U' 的基.

定义：如果 U 和 W 是域 k 上的向量空间. 它们的**直和**是指一切有序对的集合：

$$U\oplus W=\{(u,w):u\in U,w\in W\},$$

配置加法

$$(u,w)+(u',w')=(u+u',w+w')$$

和标量乘法

$$\alpha(u,w) = (\alpha u, \alpha w).$$

3.74 如果 U 和 W 是域 k 上的有限维向量空间，证明

$$\dim(U \oplus W) = \dim(U) + \dim(W).$$

3.7.2 线性变换

称两个向量空间之间的同态为线性变换.

定义 如果 V 和 W 是域 k 上的向量空间，则函数 $T: V \to W$ 称为**线性变换**，如果对一切 $u,v \in V$ 和一切标量 $a \in k$，

(i) $T(u+v) = T(u) + T(v)$;

(ii) $T(av) = aT(v)$.

我们说一个线性变换 T 是**非奇异**的（或是**同构**），如果 T 是双射．称两个向量空间 V 和 W 是**同构**的，如果存在非奇异线性变换 $T: V \to W$，记为 $V \cong W$.

如果不考虑标量乘法，则线性空间是（加法）阿贝尔群，线性变换 T 是群同态．易知 T 保持一切 k-线性组合：

171

$$T(a_1 v_1 + \cdots + a_m v_m) = a_1 T(v_1) + \cdots + a_m T(v_m).$$

例 3.91 (i) 任一向量空间 V 上的恒等函数 $1_V: V \to V$ 是非奇异线性变换.

(ii) 如果 θ 是一个角，则围绕原点旋转 θ 角是一个线性变换 $R_\theta: \mathbb{R}^2 \to \mathbb{R}^2$．函数 R_θ 保持加法，因为它把平行四边形变成平行四边形，它也保持标量乘法，因为它保持箭头的长度.

(iii) 如果 V 和 W 是域 k 上的向量空间，记 $\mathrm{Hom}_k(V,W)$ 为一切线性变换 $V \to W$ 的集合．定义加法 $S+T$ 为对一切 $v \in V, v \mapsto S(v) + T(v)$．对 $\alpha \in k$，定义标量乘法 $\alpha T: V \to W$ 为对一切 $v \in V, v \mapsto \alpha T(v)$. $S+T$ 和 αT 两者都是线性变换，从而 $\mathrm{Hom}_k(V,W)$ 是 k 上的向量空间. ■

定义 如果 V 是域 k 上的向量空间，则**一般线性群**是指一切非奇异线性变换 $V \to V$ 的集合，记为 $\mathrm{GL}(V)$.

线性变换 S 和 T 的复合 ST 也是线性变换，如果 S 和 T 都是非奇异的，则 ST 也是非奇异的，此外，非奇异线性变换的逆也是非奇异的．因为函数的复合总是结合的，所以 $\mathrm{GL}(V)$ 是以复合作为运算的群.

我们现在说明如何构造线性变换 $T: V \to W$，其中 V 和 W 是域 k 上的向量空间．下一定理说存在可随意改变基的线性变换.

定理 3.92 设 $v_1, \cdots, v_n$ 是域 k 上向量空间 V 的基．如果 W 是域 k 上的向量空间，且 $u_1, \cdots, u_n$ 是 W 中的向量表，则存在唯一的线性变换 $T: V \to W$ 使得对一切 $i, T(v_i) = u_i$.

证明 由定理 3.77，每个 $v \in V$ 可唯一地表示为 $v = \sum_i a_i v_i$ 的形式，从而由 $T(v) = \sum a_i u_i$ 给出的 $T: V \to W$ 是一个(合理定义的)函数．现在很容易验证 T 是线性变换.

为证明 T 的唯一性，假定 $S: V \to W$ 是线性变换满足对一切 i，

$$S(v_i) = u_i = T(v_i).$$

如果 $v \in V$，则 $v = \sum a_i v_i$ 且

$$S(v)=S(\sum a_iv_i)$$
$$=\sum S(a_iv_i)$$
$$=\sum a_iS(v_i)$$
$$=\sum a_iT(v_i)=T(v).$$

因 v 是任意的，所以 $S=T$. ■

系 3.93 如果两个线性变换 $S,T:V\to W$ 在基上一致，则 $S=T$.

172

证明 由本命题所定义的线性变换的唯一性立即得证. ■

容易描述定义在 k^n 上的线性变换.

命题 3.94 如果 $T:k^n\to k^m$ 是线性变换，则存在 $m\times n$ 矩阵 A 使得对一切 $y\in k^n$，

$$T(y)=Ay.$$

（这里 y 是 $n\times 1$ 列矩阵，Ay 是矩阵乘法.）

证明概要 设 $e_1,\cdots,e_n$ 是 k^n 的标准基，$e'_1,\cdots,e'_m$ 是 k^m 的标准基，定义矩阵 $A=[a_{ij}]$ 为第 j 列是 $T(e_j)$ 的坐标集. 如果 $S:k^n\to k^m$ 定义为 $S(y)=Ay$，则因为 S 和 T 在基上一致：$T(e_j)=\sum_i a_{ij}e_i=Ae_j$，所以 $S=T$. ■

命题 3.94 建立了线性变换和矩阵之间的联系，由于要应用这种构造到两个线性变换的复合上，因而产生了矩阵乘法的定义.

定义 设 $X=v_1,\cdots,v_n$ 是 V 的基，$Y=w_1,\cdots,w_m$ 是 W 的基. 如果 $T:V\to W$ 是线性变换，则 T **的矩阵**是指 $m\times n$ 矩阵 $A=[a_{ij}]$，它的第 j 列 $a_{1j},a_{2j},\cdots,a_{mj}$ 是由 w 确定的 $T(v_j)$ 的坐标集：$T(v_j)=\sum_{i=1}^{m}a_{ij}w_i$. 矩阵 A 依赖于基 X 和 Y 的选取，有必要显示它们时记为

$$A={}_Y[T]_X.$$

在 $V=W$ 的情形，我们常取基 $X=v_1,\cdots,v_n$ 和 $w_1,\cdots,w_m$ 一样. 如果 $1_V:V\to V$ 是由 $v\mapsto v$ 给出的恒等线性变换，则 ${}_X[1_V]_X$ 是 $n\times n$ **单位矩阵** I_n（常省略下标 n），其定义是

$$I=[\delta_{ij}],$$

其中 δ_{ij} 是克罗内克 δ，即 I 的对角线上的元素是 1，其他是 0. 另一方面，如果 X 和 Y 是不同的基，则 ${}_Y[1_V]_X$ 不是单位矩阵，它的列是各个 x 关于基 Y 的坐标集.

例 3.95 设 $T:V\to W$ 是线性变换，$X=v_1,\cdots,v_n$ 和 $Y=w_1,\cdots,w_m$ 分别是 V 和 W 的基. 矩阵 T 由等式

$$T(v_j)=a_{1j}w_1+a_{2j}w_2+\cdots+a_{mj}w_m$$

173

建立. 为什么下标不是倒过来的？为什么不写成

$$T(v_j)=a_{j1}w_1+a_{j2}w_2+\cdots+a_{jm}w_m?$$

考虑下面的例子. 设 A 是域 k 上的 $m\times n$ 矩阵，定义为 $T(X)=AX$ 的函数 $T:k^n\to k^m$ 是一个线性变换，其中 X 是 $n\times 1$ 列向量. 如果 $e_1,\cdots,e_n$ 和 $e'_1,\cdots,e'_m$ 分别是 k^n 和 k^m 的标准基，则矩阵乘法的定义说 $T(e_j)=Ae_j$ 是 A 的第 j 列，而

$$Ae_j=a_{1j}e'_1+a_{2j}e'_2+\cdots+a_{mj}e'_m.$$

所以和 T 相伴的矩阵就是原来的矩阵 A.

在命题 3.98 中，我们将证明矩阵的乘法来自线性变换的复合. 如果 $T:V\to W$ 有矩阵 A 而 $S:W\to U$ 有矩阵 B，则线性变换 $ST:V\to U$ 有矩阵 BA. 如果把线性变换的矩阵定义为坐标集的行而

不是列，则 ST 的矩阵将变成 AB. ■

例 3.96 （i）设 $T:\mathbb{R}^2\to\mathbb{R}^2$ 是旋转 90°，T 关于标准基 $X=(1,0),(0,1)$ 的矩阵是

$$_X[T]_X=\begin{bmatrix}0&-1\\1&0\end{bmatrix}.$$

然而，如果 $Y=(0,1),(1,0)$，则

$$_Y[T]_Y=\begin{bmatrix}0&1\\-1&0\end{bmatrix}.$$

（ii）设 k 是域，设 $T:V\to V$ 是二维向量空间上的线性变换，并假定存在某个向量 v 使得 $T(v)$ 不是 v 的标量倍. 由例3.74(iii)，对于 v 的假设说明表 $X=v,T(v)$ 线性无关，因此它是 V 的一个基［因为 $\dim(V)=2$］. 记 $v_1=v,v_2=Tv$.

我们计算 $_X[T]_X$.

$$T(v_1)=v_2,\quad T(v_2)=av_1+bv_2,$$

其中 $a,b\in k$. 由此可知

$$_X[T]_X=\begin{bmatrix}0&a\\1&b\end{bmatrix}.$$ ■

下面的命题是定理 3.92 的一个解释.

命题 3.97 *设 V 和 W 是域 k 上的向量空间，$X=v_1,\cdots,v_n$ 和 $Y=w_1,\cdots,w_m$ 分别是 V 和 W 的基. 如果记一切线性变换 $T:V\to W$ 的集合为 $\mathrm{Hom}_k(V,W)$，记一切元素在 k 中的 $m\times n$ 矩阵的集合为 $\mathrm{Mat}_{m\times n}(k)$，则函数 $\mu:T\mapsto{}_Y[T]_X$ 是双射 $\mathrm{Hom}_k(V,W)\to\mathrm{Mat}_{m\times n}(k)$.*

174

证明 给定矩阵 A，它的列定义了 W 中的向量，更详细地说，如果 A 的第 j 列是 $(a_{1j},\cdots,a_{mj})$，定义 $z_j=\sum_{i=1}^{m}a_{ij}w_i$. 根据定理 3.92，存在线性变换 $T:V\to W$ 使得 $T(v_j)=z_j$ 且 $_Y[T]_X=A$. 所以 μ 是满射.

为证明 μ 是单射，假设 $_Y[T]_X=A={}_Y[S]_X$. 因为对所有 j，A 的列确定了 $T(v_j)$ 和 $S(v_j)$，由系 3.93 得 $S=T$. ■

下一命题说明矩阵乘法的定义来自何处：两矩阵的积是复合的矩阵.

命题 3.98 *设 $T:V\to W$ 和 $S:W\to U$ 是线性变换. 选取 V 的基 $X=x_1,\cdots,x_n$, W 的基 $Y=y_1,\cdots,y_m$, U 的基 $Z=z_1,\cdots,z_\ell$，则*

$$_Z[S\circ T]_X=(_Z[S]_Y)(_Y[T]_X).$$

证明 令 $_Y[T]_X=[a_{ij}]$，从而 $T(x_j)=\sum_p a_{pj}y_p$，又令 $_Z[S]_Y=[b_{qp}]$，从而 $S(y_p)=\sum_q b_{qp}z_q$. 则

$$ST(x_j)=S(T(x_j))=S\Big(\sum_p a_{pj}y_p\Big)$$
$$=\sum_p a_{pj}S(y_p)=\sum_p\sum_q a_{pj}b_{qp}z_q=\sum_q c_{qj}z_q,$$

其中 $c_{qj}=\sum_p b_{qp}a_{pj}$. 所以，

$$_Z[ST]_X=[c_{qj}]={}_Z[S]_{Y\,Y}[T]_X.$$ ■

系 3.99 *矩阵乘法是结合的.*

证明 设 A 是 $m\times n$ 矩阵，B 是 $n\times p$ 矩阵，C 是 $p\times q$ 矩阵. 由定理 3.92，存在线性变换

$$k^q \xrightarrow{T} k^p \xrightarrow{S} k^n \xrightarrow{R} k^m$$

使得 $C=[T], B=[S], A=[R]$.

则

$$[R\circ(S\circ T)]=[R][S\circ T]=[R]([S][T])=A(BC).$$

另一方面，

$$[(R\circ S)\circ T]=[R\circ S][T]=([R][S])[T]=(AB)C.$$

因函数的复合是结合的，

$$R\circ(S\circ T)=(R\circ S)\circ T,$$

从而

$$A(BC)=[R\circ(S\circ T)]=[(R\circ S)\circ T]=(AB)C.$$ ■

也可以直接证明系 3.99，尽管十分单调乏味，但是与线性变换的复合之间的联系是矩阵乘法具有结合性的真实原因．175

系 3.100 设 $T: V\to W$ 是域 k 上向量空间 V 的线性变换，X 和 Y 分别是 V 和 W 的基．如果 T 是非奇异的，则 T^{-1} 的矩阵是 T 的矩阵的逆：

$${}_X[T^{-1}]_Y=({}_Y[T]_X)^{-1}.$$

证明 $I={}_Y[1_W]_Y={}_Y[T]_{XX}[T^{-1}]_Y$，且 $I={}_X[1_V]_X={}_X[T^{-1}]_{YY}[T]_X$. ■

下一个系确定了同一个线性变换产生的所有矩阵．

系 3.101 设 $T: V\to V$ 是域 k 上向量空间 V 的线性变换．如果 X 和 Y 都是 V 的基，则存在元素在 k 中的非奇异矩阵 P 使得

$${}_Y[T]_Y=P({}_X[T]_X)P^{-1}.$$

反之，如果 $B=PAP^{-1}$，其中 B, A, P 都是元素在 k 中的 $n\times n$ 矩阵，且 P 是非奇异的，则存在线性变换 $T: k^n\to k^n$ 和 k^n 的基 X 和 Y 使得 $B={}_Y[T]_Y, A={}_X[T]_X$．

证明 第一个陈述来自命题 3.98 和结合性：

$${}_Y[T]_Y={}_Y[1_V T 1_V]_Y=({}_Y[1_V]_X)({}_X[T]_X)({}_X[1_V]_Y).$$

令 $P={}_Y[1_V]_X$，注意到系 3.100 给出 $P^{-1}={}_X[1_V]_Y$.

关于逆命题，设 $E=e_1,\cdots,e_n$ 是 k^n 的标准基，定义 $T: k^n\to k^n$ 为 $T(e_j)=Ae_j$（记住 k^n 中的向量是列向量，从而 Ae_j 是矩阵乘法．其实，Ae_j 就是 A 的第 j 列）．由此 $A={}_E[T]_E$．现在由 $y_j=P^{-1}e_j$ 定义一个基 $Y=y_1,\cdots,y_n$，基 Y 中的向量是 P^{-1} 的列．注意，因为 P^{-1} 是非奇异的，所以 Y 是基．只需证明 $B={}_Y[T]_Y$，即 $T(y_j)=\sum_i b_{ij}y_i$，其中 $B=[b_{ij}]$.

$$\begin{aligned}T(y_j)&=Ay_j\\&=AP^{-1}e_j\\&=P^{-1}Be_j\\&=P^{-1}\sum_i b_{ij}e_i\\&=\sum_i b_{ij}P^{-1}e_i\\&=\sum_i b_{ij}y_j\end{aligned}$$ ■ 176

定义 设 A 和 B 是元素在域 k 中的两个 $n\times n$ 矩阵，如果存在元素在 k 中的非奇异矩阵 P 使得

$B = PAP^{-1}$，则称 A 和 B **相似**.

系 3.101 说两个矩阵由向量空间 V 上的同一个线性变换产生（由于基的选取不同）当且仅当它们相似. 第 9 章中我们将知道如何确定给定的两个矩阵是否相似.

和群同态、环同态一样，我们可以定义线性变换的核和象.

定义 如果 $T: V \to W$ 是线性变换，则 T 的**核**（或**零空间**）是指

$$\ker T = \{v \in V : T(v) = 0\},$$

T 的**象**是指

$$\mathrm{im} T = \{w \in W : w = T(v), \text{对某个 } v \in V\}.$$

如命题 3.94 中一样，一个元素在域 k 中的 $m \times n$ 矩阵确定了一个线性变换 $k^n \to k^m$，即 $y \mapsto Ay$，其中 y 是 $n \times 1$ 列向量，这个线性变换的核就是通常所说的 A 的解空间 [见例 3.70 (iv)].

下一命题的证明是显然的.

命题 3.102 设 $T: V \to W$ 是线性变换.

(i) $\ker T$ 是 V 的子空间，$\mathrm{im} T$ 是 W 的子空间.

(ii) T 是单射当且仅当 $\ker T = \{0\}$.

我们现在解释下述事实：域 k 上有 r 个方程、n 个未知数的齐次方程组，如果 $r < n$ 则该方程组有非平凡解. 如果该方程组的系数矩阵是 $r \times n$ 矩阵 A，则 $\varphi: x \mapsto Ax$ 是线性变换 $\varphi: k^n \to k^r$. 如果只有平凡解，则 $\ker\varphi = \{0\}$，从而 k^n 同构于 k^r 的子空间，这与系 3.90 (i) 矛盾.

引理 3.103 设 $T: V \to W$ 是线性变换.

(i) 如果 T 是非奇异的，则对于 V 的每个基 $X = v_1, \cdots, v_n$，$T(X) = T(v_1), T(v_2), \cdots, T(v_n)$ 是 W 的一个基.

(ii) 反之，如果存在 V 的某个基 $X = v_1, \cdots, v_n$ 使得 $T(X) = T(v_1), T(v_2), \cdots, T(v_n)$ 是 W 的基，则 T 是非奇异的.

证明 (i) 如果 $\sum c_i T(v_i) = 0$，则 $T(\sum c_i v_i) = 0$，从而 $\sum c_i v_i \in \ker T = \{0\}$. 因 X 线性无关，所以每个 $c_i = 0$. 如果 $w \in W$，则因 T 是满射，所以存在 $v \in V$ 使得 $w = T(v)$. 但 $v = \sum a_i v_i$，因此 $w = T(v) = T(\sum a_i v_i) = \sum a_i T(v_i)$. 所以 $T(X)$ 是 W 的基.

177

(ii) 设 $w \in W$. 因 $T(v_1), \cdots, T(v_n)$ 是 W 的基，所以有 $w = \sum c_i T(v_i) = T(\sum c_i v_i)$，从而 T 是满射. 如果 $\sum c_i v_i \in \ker T$，则 $\sum c_i T(v_i) = 0$，从而由线性无关性得所有 $c_i = 0$，因此 $\sum c_i v_i = 0$ 且 $\ker T = \{0\}$. 所以 T 是非奇异的. ■

定理 3.104 如果 V 是域 k 上的 n 维向量空间，则 V 同构于 k^n.

证明 选取 V 的基 $v_1, \cdots, v_n$. 如果 $e_1, \cdots, e_n$ 是 k^n 的标准基，则定理 3.92 说存在线性变换 $T: V \to k^n$ 使得对一切 i，$T(v_i) = e_i$，根据引理 3.103，T 是非奇异的. ■

定理 3.104 不只是说每个有限维向量空间本质上就是熟知的一切 n 元组的向量空间，它还说明 V 中基的选取相当于 V 中对每个向量的坐标集的选取. 由于常用的坐标对于给定的问题或许并不是最合适的，所以可以自由地改变坐标，如读者可能已经看到的（在微积分课程中）旋转坐标轴可以简化圆锥截线的方程.

系 3.105 域 k 上两个有限维向量空间 V 和 W 同构当且仅当 $\dim(V) = \dim(W)$.

注 在定理 6.51 中，我们会看到这个系对于无限维向量空间也成立.

证明 假定存在非奇异的 $T: V \to W$. 如果 $X = v_1, \cdots, v_n$ 是 V 的基，则由引理 3.103 知，

$T(v_1),\cdots,T(v_n)$ 是 W 的基．所以 $\dim(W)=|X|=\dim(V)$．

如果 $n=\dim(V)=\dim(W)$，则由定理 3.104，存在同构 $T:V\to k^n$ 和 $S:W\to k^n$，从而复合 $S^{-1}T:V\to W$ 是非奇异的．■

命题 3.106　*设 V 是有限维向量空间满足 $\dim(V)=n$，又设 $T:V\to V$ 是线性变换．下列陈述等价：*

（ⅰ）T 是同构；

（ⅱ）T 是满射；

（ⅲ）T 是单射．

证明　（ⅰ）⇒（ⅱ）显然成立．

（ⅱ）⇒（ⅲ）设 $v_1,\cdots,v_n$ 是 V 的基．因 T 是满射，存在向量 $u_1,\cdots,u_n$ 使得对一切 i，$Tu_i=v_i$．我们断言 $u_1,\cdots,u_n$ 线性无关．如果存在不全为零的标量 $c_1,\cdots,c_n$ 使得 $\sum c_iu_i=0$，则导出一个相关关系 $0=\sum c_iT(u_i)=\sum c_iv_i$，从而产生矛盾．由系 3.89（ⅱ），$u_1,\cdots,u_n$ 是 V 的基．为证明 T 是单射，只需证明 $\ker T=\{0\}$．假设 $T(v)=0$．现在 $v=\sum c_iu_i$，因此 $0=T\sum c_iu_i=\sum c_iv_i$，因而 $v_1,\cdots,v_n$ 线性无关给出一切 $c_i=0$，从而 $v=0$．所以 T 是单射．

178

（ⅲ）⇒（ⅰ）设 $v_1,\cdots,v_n$ 是 V 的基．如果 $c_1,\cdots,c_n$ 是不全为零的标量，则因为基线性无关，$\sum c_iv_i\neq 0$．因 T 是单射，有 $\sum c_iTv_i\neq 0$，从而 $Tv_1,\cdots,Tv_n$ 线性无关．因此引理 3.103（ⅱ）证明 T 是同构．■

回忆元素在域 k 中的 $n\times n$ 矩阵 A 是非奇异的，如果存在元素在 k 中的矩阵 B（A 的逆）使得 $AB=I=BA$．下一个系证明“单边有逆”就够了．

系 3.107　*如果 A 和 B 是 $n\times n$ 矩阵满足 $AB=I$，则 $BA=I$．所以 A 是非奇异的，且 B 是 A 的逆．*

证明　存在线性变换 $T,S:k^n\to k^n$ 使得 $[T]=A,[S]=B$．$AB=I$ 给出

$$[TS]=[T][S]=[1_{k^n}].$$

根据命题 3.97，因为 $T\mapsto[T]$ 是双射，从而 $TS=1_{k^n}$．由命题 1.47，T 是满射，S 是单射．但命题 3.106 证明 T 和 S 两者都是同构，于是 $S=T^{-1}$ 且 $TS=1_{k^n}=ST$，所以正如要证的 $I=[ST]=[S][T]=BA$．■

定义　*元素在域 k 中的一切非奇异 $n\times n$ 矩阵的集合记为 $\mathrm{GL}(n,k)$．*

我们已经证明了结合性，所以容易证明 $\mathrm{GL}(n,k)$ 在矩阵乘法下是群．

基的一个选取给出一般线性群和非奇异的矩阵群之间一个同构．

命题 3.108　*设 V 是域 k 上的 n 维向量空间，$X=v_1,\cdots,v_n$ 是 V 的基．定义 $\mu:\mathrm{GL}(V)\to\mathrm{GL}(n,k)$ 为 $T\mapsto[T]={}_X[T]_X$，则 μ 是同构．*

证明　由命题 3.97，函数 $\mu':T\mapsto[T]={}_X[T]_X$ 是双射

$$\mathrm{Hom}_k(V,V)\to\mathrm{Mat}_n(k),$$

其中 $\mathrm{Hom}_k(V,V)$ 表示 V 上一切线性变换的集合，$\mathrm{Mat}_n(k)$ 表示元素在 k 中的一切 $n\times n$ 矩阵的集合．此外，命题 3.98 说明对一切 $T,S\in\mathrm{Hom}_k(V,V)$，$[TS]=[T][S]$．

如果 $T\in\mathrm{GL}(V)$，则根据系 3.100，$[T]$ 是非奇异矩阵；即如果 μ 是 μ' 的限制，则 $\mu:\mathrm{GL}(V)\to\mathrm{GL}(n,k)$ 是单同态．

179

剩下的是证明 μ 是满射．如果 $A\in\mathrm{GL}(n,k)$，则对某个 $T:V\to V$ 有 $A=[T]$．只需证明 T 是同构；即 $T\in\mathrm{GL}(V)$．因 $[T]$ 是非奇异矩阵，存在矩阵 B 使得 $[T]B=I$．现在对某个 $S:V\to V$ 有

$B=[S]$，且
$$[TS]=[T][S]=I=[1_V].$$
因 μ 是双射，所以 $TS=1_V$，由系 3.107，$T\in \mathrm{GL}(V)$. ■

容易确定一般线性群的中心，我们现在推广习题 2.56.

定义 线性变换 $T: V\to V$ 称为**标量**变换，如果存在 $c\in k$ 使得对一切 $v\in V, T(v)=cv$，即 $T=c1_V$. **标量矩阵**是指形为 cI 的矩阵，其中 $c\in k$，I 是单位矩阵.

一个标量变换 $T=c1_V$ 是非奇异的当且仅当 $c\neq 0$（它的逆是 $c^{-1}1_V$）.

系 3.109 （ⅰ）群 $\mathrm{GL}(V)$ 的中心由一切非奇异标量变换组成.

（ⅱ）群 $\mathrm{GL}(n,k)$ 的中心由一切非奇异标量矩阵组成.

证明 （ⅰ）如果 $T\in \mathrm{GL}(V)$ 不是标量变换，则例3.96（ⅱ）证明存在 $v\in V$ 使得 $v, T(v)$ 线性无关. 由命题 3.87，存在 V 的基 $v, T(v), u_3, \cdots, u_n$. 易知 $v, v+T(v), u_3, \cdots, u_n$ 也是 V 的基，由此存在非奇异线性变换 S 使得 $S(v)=v, S(T(v))=v+T(v)$，以及对一切 i. $S(u_i)=u_i$. 现在因为 $ST(v)=v+T(v)$ 而 $TS(v)=T(v)$，因此 S 和 T 不可交换. 所以 T 不在 $\mathrm{GL}(V)$ 的中心.

（ⅱ）如果 $f: G\to H$ 是群 G 和 H 之间的任意一个群同构，则 $f(Z(G))=Z(H)$. 特别地，如果 $T=c1_V$ 是非奇异标量变换，则 $[T]$ 在 $\mathrm{GL}(n,k)$ 的中心，但容易验证 $[T]=cI$ 是标量矩阵. ■

习题

3.75 设 V 和 W 是域 k 上的向量空间，$S, T: V\to W$ 是线性变换.

（ⅰ）如果 V 和 W 是有限维的，证明
$$\dim(\mathrm{Hom}_k(V,W))=\dim(V)\dim(W).$$

（ⅱ）定义域 k 上的向量空间 V 的**对偶空间** V^* 为
$$V^*=\mathrm{Hom}_k(V,k).$$

180

如果 $\dim(V)=n$，证明 $\dim(V^*)=n$，因此 $V^*\cong V$.

（ⅲ）如果 $X=v_1,\cdots,v_n$ 是 V 的基，定义 $\delta_1,\cdots,\delta_n\in V^*$ 为
$$\delta_i(v_j)=\begin{cases}0 & 当\ j\neq i\\ 1 & 当\ j=i.\end{cases}$$

证明 $\delta_1,\cdots,\delta_n$ 是 V^* 的基（叫做由 $v_1,\cdots,v_n$ 形成的**对偶基**）.

3.76 如果 $A=\begin{bmatrix}a & b\\ c & d\end{bmatrix}$，定义 $\det(A)=ad-bc$. 如果 V 是有基 $X=v_1, v_2$ 的向量空间，定义 $T: V\to V$ 为 $T(v_1)=av_1+bv_2, T(v_2)=cv_1+dv_2$. 证明 T 是非奇异线性变换当且仅当 $\det({}_X[T]_X)\neq 0$.

提示：可以假定线性代数的下列（容易证明的）事实：给定系数在一个域上的线性方程组，
$$ax+by=p$$
$$cx+dy=q,$$
则存在唯一解当且仅当 $ad-bc\neq 0$.

3.77 设 U 是向量空间 V 的子空间.

（ⅰ）证明由 $v\mapsto v+U$ 给出的**自然映射** $\pi: V\to V/U$ 是核为 U 的线性变换.（习题 3.71 中定义了商空间.）

（ⅱ）对向量空间陈述并证明**第一同构定理**.

提示：命题的陈述是：如果 $f: V\to W$ 是 $\ker f=U$ 的线性变换，则 U 是 V 的子空间，且存在同构 $\varphi: V/U\cong \mathrm{im} f$ 即 $\varphi(v+U)=f(v)$.

3.78　设 V 是域 k 上的有限维向量空间，记$\mathcal{B}$为 V 的一切基的族．证明$\mathcal{B}$是传递的 $\mathrm{GL}(V)$ - 集．

提示：用定理 3.92.

3.79　（ⅰ）如果 U 和 W 是向量空间 V 的子空间满足 $U \cap W = \{0\}$ 和 $U + W = V$．证明 $V \cong U \oplus W$（见直和的定义）．

（ⅱ）向量空间 V 的子空间 U 称为**直和项**，如果存在 V 的子空间 W 使得 $U \cap W = \{0\}, U+W=V$．如果 V 是域 k 上的有限维向量空间，证明每个子空间 U 都是一个直和项．

提示：取 U 的基 X，把它扩张为 V 的基 X'，定义 $W = \langle X' - X \rangle$．

3.80　如果 $T: V \to W$ 是域 k 上向量空间之间的线性变换，定义 T 的**秩**$\mathrm{rank}(T)$为

$$\mathrm{rank}(T) = \dim(\mathrm{im}T).$$

（ⅰ）把 $m \times n$ 矩阵 A 的列看作 m 元组，定义 A 的**列空间**为列张成的子空间 k^m，定义 A 的**秩**$\mathrm{rank}(A)$为列空间的维数．如果 $T: k^n \to k^m$ 是由 $T(X) = AX$ 定义的线性变换，其中 X 是$n \times 1$ 向量，证明

$$\mathrm{rank}(A) = \mathrm{rank}(T).$$

（ⅱ）如果 A 是 $m \times n$ 矩阵，B 是 $p \times m$ 矩阵，证明

$$\mathrm{rank}(BA) \leqslant \mathrm{rank}(A).$$

（ⅲ）证明相似的 $n \times n$ 矩阵有相同的秩．

181

3.8　商环和有限域

我们回到交换环．代数基本定理（定理 4.49）指出 $\mathbb{C}[x]$ 中的每个非常数多项式是 $\mathbb{C}[x]$ 中的一次多项式的积，即$\mathbb{C}$包含了 $\mathbb{C}[x]$ 中每个多项式的所有的根．我们要证明任意域 k 上关于多项式的类似于代数基本定理的一种“局部”情形：给定多项式 $f(x) \in k[x]$，则存在包含 k 的某个域 K，它也包含 $f(x)$ 的所有的根．（我们把它称为局部类似，这是因为更大域 K 虽然包含多项式 $f(x)$ 的所有的根，但它有可能不包含 $k[x]$ 中其他多项式的根）．隐含于 K 的结构中的主要思想涉及商环，它是一种类似于商群的结构．

设 I 是交换环 R 的理想．如果我们忘掉乘法，则 I 是加法群 R 的子群．因 R 是阿贝尔群，子群 I 必定是正规子群，从而商群 R/I 有定义，正如由 $\pi(a) = a + I$ 给出的自然映射 $\pi: R \to R/I$ 也有定义．回忆引理2.40(ⅰ)，我们现在用加法记号表示：在 R/I 中，$a+I=b+I$ 当且仅当 $a-b \in I$．

定理 3.110　*如果 I 是交换环 R 的理想，则加法阿贝尔群 R/I 可以形成这样一个交换环，它使得自然映射 $\pi: R \to R/I$ 是满射环同态．*

证明概要　在加法阿贝尔群 R/I 上定义乘法为

$$(a+I)(b+I) = ab+I.$$

为了证明这是合理定义的函数 $R/I \times R/I \to R/I$，假定 $a+I = a'+I$ 和 $b+I = b'+I$；即 $a-a' \in I, b-b' \in I$．我们必须证明 $(a'+I)(b'+I) = a'b'+I = ab+I$，即 $ab-a'b' \in I$．但

$$\begin{aligned} ab-a'b' &= ab-a'b+a'b-a'b' \\ &= (a-a')b+a'(b-b') \in I, \end{aligned}$$

正如所要的．

为验证 R/I 是交换环，现在只需证明乘法的结合性、交换性、分配性，以及 1 是$1+I$．这些性质的证明都很简单，因为它们继承自 R 中的相应性质．例如，R/I 中的乘法是交换的，这是因为

$$(a+I)(b+I) = ab+I = ba+I = (b+I)(a+I).$$

把等式 $(a+I)(b+I)=ab+I$ 用 π 的定义重新写出来，也就是 $a+I=\pi(a)$，得到 $\pi(a)\pi(b)=\pi(ab)$．因 $\pi(1)=1+I$，从而 π 是环同态．最后，因 $a+I=\pi(a)$，π 是满射． ■

182

定义 定理 3.110 中构造的交换环 R/I 称为 R 模 I（简记为 $R\bmod I$）的**商环**.[⊖]

我们在例 2.68 中看到加法阿贝尔群 $\mathbb{Z}/(m)$ 等同于 $\mathbb{I}_m$. 它们有相同的元素：陪集 $a+(m)$ 和同余类 $[a]$ 是 $\mathbb{Z}$ 的同一子集；它们有相同的加法：

$$a+(m)+b+(m)=a+b+(m)=[a+b]=[a]+[b].$$

现在还可以看到商环 $\mathbb{Z}/(m)$ 和交换环 $\mathbb{I}_m$ 一致，因为两个乘法也一致：

$$(a+(m))(b+(m))=ab+(m)=[ab]=[a][b].$$

现在可以证明命题 3.50 的逆．

系 3.111 如果 I 是交换环 R 中的理想，则存在交换环 A 和环同态 $\pi: R\to A$ 使得 $I=\ker\pi$.

证明 如果忘掉乘法，则自然映射 $\pi: R\to R/I$ 是加法群之间的同态，由系 2.69，

$$I=\ker\pi=\{r\in R: \pi(a)=0+I=I\}.$$

现在回忆乘法：$(a+I)(b+I)=ab+I$，即 $\pi(a)\pi(b)=\pi(ab)$．所以 π 是环同态，且无论把 π 看作环同态还是加法群的同态，$\ker\pi$ 都等于 I. ■

定理 3.112（第一同构定理） 如果 $f: R\to A$ 是环的同态，则 $\ker f$ 是 R 中的理想，$\operatorname{im} f$ 是 A 的子环，且

$$R/\ker f\cong \operatorname{im} f.$$

证明 设 $I=\ker f$. 在命题 3.50 中我们已经看到 I 是 R 中的理想，$\operatorname{im} f$ 是 A 的子环．

如果忘掉环中的乘法，则定理 2.70 的证明表明由 $\varphi(r+I)=f(r)$ 给出的函数 $\varphi: R/I\to\operatorname{im} f$ 是加法群的同态．因 $\varphi(1+I)=f(1)=1$，只需证明 φ 保持乘法．而

$\varphi((r+I)(s+I))=\varphi(rs+I)=f(rs)=f(r)f(s)=\varphi(r+I)\varphi(s+I)$．所以 φ 是环同态． ■

对于环如同对于群一样，第一同构定理从一个我们已知其核和象的同态出发构造了一个同构. 它也说明在商环和同态的象之间没有显著的差别．对于交换环也有类似于群的第二和第三同构定理（第三同构定理见习题 3.82，第二同构定理在模的课文中有很好的陈述，见定理 7.9），但是它们对于环不像在群中那么有用．然而有一个有用的和对应定理类似的定理，我们在后面证明它（见命题 6.1）．

183

定义 如果 k 是域，则 k 的一切子域的交称为 k 的**素域**.

$\mathbb{C}$ 的每个子域包含$\mathbb{Q}$，从而$\mathbb{C}$ 和$\mathbb{R}$ 的素域是$\mathbb{Q}$. 有限域的素域恰好是整数 $\bmod p$，我们在下面给予证明．

记号 从现在起，当我们把$\mathbb{I}_p$ 看作域时，记 $\mathbb{I}_p$ 为$\mathbb{F}_p$．

借用群论的术语，称一个域的包含子集 X 的一切子域的交为 *X 生成的子域*．它在如下的意义下是包含 X 的最小的子域：如果 F 是包含 X 的任意子域，则 F 包含 X 生成的子域．素域是 1 生成的子域，$\mathbb{F}_p(x)$ 的素域是$\mathbb{F}_p$.

命题 3.113 如果 k 是域，则它的素域同构于$\mathbb{Q}$ 或$\mathbb{F}_p$，其中 p 是某个素数．

证明 记 k 中的 1 为 ε，考虑由 $\chi(n)=n\varepsilon$ 定义的环同态 $\chi:\mathbb{Z}\to k$. 因$\mathbb{Z}$ 中的每个理想都是主理想，存在整数 m 使得 $\ker\chi=(m)$．如果 $m=0$，则 χ 是单射，从而存在$\mathbb{Z}$ 的一个同构复制是 k 的子

⊖ 推测所以叫它商环是因为它和商群类似．

环．由习题 3.47（ii），存在域 $Q \cong \mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$ 使得 $\mathrm{im}\chi \subseteq Q \subseteq k$．现在 Q 是 k 的素域，这是因为 k 的每个子域包含 1，因此包含 $\mathrm{im}\chi$，又因为 $Q \cong \mathbb{Q}$ 没有真子域，因此包含 Q. 如果 $m \neq 0$，则第一同构定理给出 $\mathbb{I}_m = \mathbb{Z}/(m) \cong \mathrm{im}\chi \subseteq k$．因 k 是域，因此 $\mathrm{im}\chi$ 是整环，从而由命题 3.6 得 m 为素数．如果现在把 m 写成 p，则 $\mathrm{im}\chi = \{0, \varepsilon, 2\varepsilon, \cdots, (p-1)\varepsilon\}$ 是 k 的同构于 $\mathbb{F}_p$ 的子域．显然，每个子域包含 ε 并因此包含 $\mathrm{im}\chi$，从而 $\mathrm{im}\chi$ 是 k 的素域． ■

上面的结果是对域进行分类的第一步．

定义 如果域 k 的素域同构于 $\mathbb{Q}$，则称 k 具有**特征 0**；如果域 k 的素域同构于 $\mathbb{F}_p$，其中 p 是某个素数，则称 k 具有**特征 p**.

域 $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ 具有特征 0，如它们的任何子域一样；每个有限域有特征 p，p 是某个素数，和 $\mathbb{F}_p$ 上的一切有理函数环 $\mathbb{F}_p(x)$ 一样．

命题 3.114 如果 k 是特征 $p > 0$ 的域，则对一切 $a \in k, pa = 0$．

证明 因 k 有特征 p，有 $p \cdot 1 = 0$，其中 1 是 k 中的 1. 现在从命题3.2(v)可得结论． ■

命题 3.115 如果 k 是有限域，则对于某个素数 p 和 $n \geq 1$，$|k| = p^n$．

证明 k 的素域 P 不可能是无限域 $\mathbb{Q}$，从而对某个素数 p 有 $P \cong \mathbb{F}_p$．现在 k 是 P 上的向量空间，所以 k 是 $\mathbb{F}_p$ 上的向量空间．显然 k 是有限维的，如果 $\dim \mathbb{F}_p(k) = n$，则 $|k| = p^n$． ■ [184]

注 这里用群论来证明上一命题．假定 k 是有限域，它的阶 $|k|$ 可被不同的素数 p 和 q 整除．由命题 2.78，即阿贝尔群的柯西定理，在 k 中存在元素 a 和 b，它们的阶分别为 p 和 q. 如果记 k 中的 1 为 ε，则元素 $p\varepsilon$（p 个 ε 的和）和 $q\varepsilon$ 满足 $(p\varepsilon)a = 0$ 及 $(q\varepsilon)b = 0$．因 k 是域，它必是整环，所以

$$p\varepsilon = 0 = q\varepsilon.$$

但 $(p, q) = 1$，从而存在整数 s 和 t 使得 $sp + tq = 1$．因此，$\varepsilon = s(p\varepsilon) + t(q\varepsilon) = 0$，出现矛盾．所以 $|k|$ 只有一个素因数，比如 p，从而 $|k|$ 是 p 的幂．

命题 3.116 如果 k 是域，且 $I = (p(x))$，其中 $p(x)$ 是 $k[x]$ 中的非零多项式，那么下面的陈述等价：$p(x)$ 是不可约的；$k[x]/I$ 是域；$k[x]/I$ 是整环．

证明 假定 $p(x)$ 是不可约的．注意到 $I = (p(x))$ 是真理想，从而 $k[x]/I$ 中的 1 就是 $1+I$，它不等于零．如果 $f(x) + I \in k[x]/I$ 非零，则 $f(x) \notin I$，即 $f(x)$ 不是 $p(x)$ 的倍数，换句话说，$p \nmid f$．由引理 3.36，p 和 f 互素，从而存在多项式 s 和 t 使得 $sf + tp = 1$．于是 $sf - 1 \in I$ 且 $1 + I = sf + I = (s+I)(f+I)$．所以 $k[x]/I$ 的每个非零元素都有逆，从而 $k[x]/I$ 是域．

当然，每个域都是整环．

如果 $k[x]/I$ 是整环．如果 $p(x)$ 不是 $k[x]$ 中的不可约多项式，则存在 $k[x]$ 中的因式分解 $p(x) = g(x)h(x)$，其中 $\deg(g) < \deg(p), \deg(h) < \deg(p)$．由此，$g(x) + I$ 和 $h(x) + I$ 在 $k[x]/I$ 中都不是零．毕竟 $k[x]/I$ 中的零是 $0 + I = I$，且 $g(x) + I = I$ 当且仅当 $g(x) \in I = (p(x))$；如果真的这样，则 $p(x) \mid g(x)$，与 $\deg(p) \leqslant \deg(g)$ 矛盾．乘积

$$(g(x) + I)(h(x) + I) = p(x) + I = I$$

在商环中是零，此与 $k[x]/I$ 是整环矛盾．所以 $p(x)$ 必定是一个不可约多项式． ■

R/I 的结构可能比较复杂，但是对于特定选取的 R 和 I，可以容易地描述交换环 R/I．例如当 $p(x)$ 是不可约多项式时，下面的命题给出域 $k[x]/(p(x))$ 的完整描述．

命题 3.117 设 k 是域，设 $p(x) \in k[x]$ 是 d 次首一不可约多项式．令 $K = k[x]/I$，其中 $I = (p(x))$ 又令 $\beta = x + I \in K$．

（i）K 是域，且 $k' = \{a + I : a \in k\}$ 是 K 的同构于 k 的子域．所以，如果把 k' 等同于 k，则 k 是 K 的子域．

185

（ii）β 是 $p(x)$ 在 K 中的一个根．

（iii）如果 $g(x) \in k[x]$ 且 β 是 $g(x)$ 的根，则在 $k[x]$ 中 $p(x) \mid g(x)$．

（iv）$p(x)$ 是 $k[x]$ 中唯一的以 β 为根的首一不可约多项式．

（v）表 $1, \beta, \beta^2, \cdots, \beta^{d-1}$ 是 K 作为 k 上的向量空间的基，从而 $\dim_k(K) = d$．

证明 （i）因为 $p(x)$ 是不可约的，根据命题 3.116，商环 $K = k[x]/I$ 是域．用系 3.53，易知由 $\varphi(a) = a + I$ 定义的自然映射的限制 $\varphi = \pi \mid k : k \to K$ 是 $k \to k'$ 的同构．

（ii）设 $p(x) = a_0 + a_1 x + \cdots + a_{d-1}x^{d-1} + x^d$，其中对一切 $i, a_i \in k$. 在 $K = k[x]/I$ 中，因为 $p(x) \in I = (p(x))$，有

$$\begin{aligned} p(\beta) &= (a_0 + I) + (a_1 + I)\beta + \cdots + (1 + I)\beta^d \\ &= (a_0 + I) + (a_1 + I)(x + I) + \cdots + (1 + I)(x + I)^d \\ &= (a_0 + I) + (a_1 x + I) + \cdots + (1x^d + I) \\ &= a_0 + a_1 x + \cdots + x^d + I \\ &= p(x) + I = I, \end{aligned}$$

但 $I = 0 + I$ 是 $K = k[x]/I$ 的零元，从而 β 是 $p(x)$ 的根．

（iii）如果在 $k[x]$ 中，$p(x) \nmid g(x)$，则因为 $p(x)$ 是不可约的，所以它们的 gcd 是 1. 因此存在 $s(x), t(x) \in k[x]$ 使得 $1 = s(x)p(x) + t(x)g(x)$．因 $k[x] \subseteq K[x]$，可以把该等式看作 $K[x]$ 中的等式．计算在 β 处的值得矛盾 1=0.

（iv）设 $h(x) \in k[x]$ 是以 β 为根的首一不可约多项式．由（iii），$p(x) \mid h(x)$. 因 $h(x)$ 不可约，所以有某个常数 c 使得 $h(x) = cp(x)$．因 $h(x)$ 和 $p(x)$ 都是首一多项式，从而 $c = 1$ 且 $h(x) = p(x)$．

（v）K 中的元素都形如 $f(x) + I$，其中 $f(x) \in k[x]$. 由带余除法，存在多项式 $q(x), r(x) \in k[x]$ 使得 $f(x) = q(x)p(x) + r(x)$，且 $r(x) = 0$ 或 $\deg(r) < d = \deg(p)$．因 $f - r = qp \in I$，从而 $f(x) + I = r(x) + I$．如果 $r(x) = b_0 + b_1 x + \cdots + b_{d-1}x^{d-1}$，其中对一切 $i, b_i \in k$，则和（ii）的证明一样，有 $r(x) + I = b_0 + b_1\beta + \cdots + b_{d-1}\beta^{d-1}$．所以 $1, \beta, \beta^2, \cdots, \beta^{d-1}$ 张成 K.

为证明唯一性，假设

$$b_0 + b_1\beta + \cdots + b_{d-1}\beta^{n-1} = c_0 + c_1\beta + \cdots + c_{d-1}\beta^{d-1}.$$

定义 $g(x) \in k[x]$ 为 $\sum_{i=0}^{d-1}(b_i - c_i)x^i$．如果 $g(x) = 0$，结论已经成立．如果 $g(x) \neq 0$，则 $\deg(g)$ 有定义，且 $\deg(g) < d = \deg(p)$．另一方面，β 是 $g(x)$ 的根，所以（iii）给出 $p(x) \mid g(x)$，因此 $\deg(p) \leqslant \deg(g)$，导致矛盾．由此 $1, \beta, \beta^2, \cdots, \beta^{d-1}$ 是 k 上的向量空间 K 的基，且有 $\dim_k(K) = d$． ■

186

定义 如果 K 是包含 k 并把它作为子域的域，则称 K 是 k 的一个（域）**扩张**，并写作“K/k 是一个域扩张”．⊖

称域 k 的一个扩域 K 为 k 的**有限扩张**，如果 K 是 k 上的有限维向量空间．称 K 的维数为 K/k

⊖ 不要把这个记号和商环的记号相混淆，因为域 K 没有值得关注的理想，特别地，如果 $k \subsetneq K$，则 k 不是 K 中的理想.

的**次数**，记为$[K:k]$.

命题 3.117（v）说明了为什么要把$[K:k]$叫做域扩张K/k的次数.

例 3.118　多项式$x^2+1\in\mathbb{R}[x]$是不可约的，从而$K=\mathbb{R}[x]/(x^2+1)$是次数为 2 的域扩张$K/\mathbb{R}$. 如果β是x^2+1的根，则$\beta^2=-1$. 此外，K的每个元素有唯一的表达式$a+b\beta$，其中$a,b\in\mathbb{R}$. 显然这是$\mathbb{C}$的另一种构造法（我们已经把它看作配置了某种加法和乘法的平面上的点）.

下面是构造同构$K\to\mathbb{C}$的自然方式. 考虑由$\varphi: f(x)\mapsto f(\mathrm{i})$给出的赋值映射$\varphi:\mathbb{R}[x]\to\mathbb{C}$. 首先，$\varphi$是满射，这是因为$a+\mathrm{i}b=\varphi(a+bx)\in\mathrm{im}\varphi$. 其次，$\ker\varphi=\{f(x)\in\mathbb{R}[x]: f(\mathrm{i})=0\}$，它是$\mathbb{R}[x]$中以 i 为根的一切多项式的集合. 我们知道$x^2+1\in\ker\varphi$，所以$(x^2+1)\subseteq\ker\varphi$. 关于反包含，取$g(x)\in\ker\varphi$. 现在 i 是$g(x)$的根，从而在$\mathbb{C}[x]$中$\gcd(g,x^2+1)\neq 1$，因此在$\mathbb{R}[x]$中$\gcd(g,x^2+1)\neq 1$. x^2+1在$\mathbb{R}[x]$中的不可约性给出$x^2+1\mid g(x)$，从而$g(x)\in(x^2+1)$，所以$\ker\varphi=(x^2+1)$. 现在第一同构定理给出$\mathbb{R}[x]/(x^2+1)\cong\mathbb{C}$. ■

在$\mathbb{C}$中作乘法最容易的方法是先把 i 当作变量然后利用条件$\mathrm{i}^2=-1$. 为计算$(a+b\mathrm{i})(c+d\mathrm{i})$，先写出$ac+(ad+bc)\mathrm{i}+bd\mathrm{i}^2$，然后注意$\mathrm{i}^2=-1$. 更一般地，如果$\beta$是不可约多项式$p(x)\in k[x]$的根，则在商环$k[x]/(p(x))$中做乘法

$$(b_0+b_1\beta+\cdots+b_{n-1}\beta^{n-1})(c_0+c_1\beta+\cdots+c_{n-1}\beta^{n-1})$$

的正确方法是把两个因式都看作β的多项式，把它们相乘，然后利用条件$p(\beta)=0$.

对域分类的第一步涉及它们的特征，即描述素域. 第二步是考虑素域上的元素是否是代数的.

定义　*设K/k是一个域扩张. 元素$\alpha\in K$称为k上的***代数元素***，如果存在某个非零多项式$f(x)\in k[x]$以α为根. 否则称α为k上的***超越元素***. 如果每个$\alpha\in K$都是k上的代数元素，则称扩张K/k为***代数扩张***.

一个实数被称为超越数时，常指它是$\mathbb{Q}$上的超越元素.

命题 3.119　*如果K/k是一个有限域扩张，则K/k是一个代数扩张.*

187

证明　由定义，K/k是有限扩张是指$[K:k]=n<\infty$，即K作为k上的向量空间有维数n. 由系 3.88，$n+1$个向量的表$1,\alpha,\alpha^2,\cdots,\alpha^n$线性相关，因此存在不全为零的$c_0,c_1,\cdots,c_n\in k$使得$\sum c_i\alpha^i=0$. 于是多项式$f(x)=\sum c_ix^i$是非零多项式，且$\alpha$是$f(x)$的根. 所以$\alpha$是$k$上的代数元素. ■

上一命题的逆命题不真. 在例 6.55 中将看到，一切在$\mathbb{Q}$上成为代数数的复数集合是$\mathbb{Q}$的一个代数扩张，它不是有限扩张.

定义　*如果K/k是一个扩张且$\alpha\in K$，则$k(\alpha)$是K的包含k和α的一切子域的交，称$k(\alpha)$为K的***添加***α到k得到的子域.*

更一般地，如果A（可以无限）是K的子集，定义$k(A)$为K的包含$k\cup A$的一切子域的交，称$k(A)$为K的**添加**A到k得到的子域. 特别地，如果$A=\{z_1,\cdots,z_n\}$是有限子集，则可以记$k(A)$为$k(z_1,\cdots,z_n)$.

显然，$k(A)$是K的包含k和A的最小子域；就是说，如果B是任意一个K的包含k和A的子域，则$k(A)\subseteq B$.

现在证明域$k[x]/(p(x))$（其中$p(x)\in k[x]$是不可约的）与根的添加具有密切的关系.

定理 3.120　*（i）如果K/k是一个域扩张且$\alpha\in K$是k上的代数元素，则存在唯一的首一不*

可约多项式 $p(x) \in k[x]$ 以 α 为根．此外，如果 $I=(p(x))$，则 $k[x]/I \cong k(\alpha)$．事实上，存在同构

$$\varphi: k[x]/I \to k(\alpha)$$

使得 $\varphi(x+I)=\alpha$，且对一切 $c \in k, \varphi(c+I)=c$．

（ⅱ）如果 $\alpha' \in K$ 是 $p(x)$ 的另一个根，则存在同构

$$\theta: k(\alpha) \to k(\alpha')$$

使得 $\theta(\alpha)=\alpha'$，且对一切 $c \in k, \theta(c)=c$.

证明 （ⅰ）考虑由赋值函数

$$\varphi: f(x) \mapsto f(\alpha)$$

定义的环同态 $\varphi: k[x] \to K$．现在 $\operatorname{im}\varphi$ 是由 α 的一切多项式组成的 K 的子环，即一切形如 $f(\alpha)$ 的元素，其中 $f(x) \in k[x]$．现在 $\ker\varphi$ 是一切以 α 为根的 $f(x) \in k[x]$ 组成的 $k[x]$ 中的理想．因 $k[x]$ 中的每个理想都是主理想，所以有某个首一多项式 $p(x) \in k[x]$ 使得 $\ker\varphi=(p(x))$．但 $k[x]/(p(x)) \cong$ 188 $\operatorname{im}\varphi$，它是整环，从而由命题 3.116，$p(x)$ 是不可约的．同一命题还说 $k[x]/(p(x))$ 是域，从而第一同构定理给出 $k[x]/(p(x)) \cong \operatorname{im}\varphi$，即 $\operatorname{im}\varphi$ 是包含 k 和 α 的 K 的子域．因为 K 的每个包含 k 和 α 的子域必包含 $\operatorname{im}\varphi$，从而 $\operatorname{im}\varphi=k(\alpha)$．我们已经证明了所有的陈述除了 $p(x)$ 的唯一性，而这一点可由命题3.117(ⅳ)得到．

（ⅱ）如同（ⅰ），存在同构 $\varphi: k[x]/I \to k(\alpha)$ 和 $\psi: k[x]/I \to k(\alpha')$ 使得对一切 $c \in k$ 有 $\varphi(c+I)=c$ 和 $\psi(c)=c+I$；而且 $\varphi: x+I \mapsto \alpha, \psi: x+I \mapsto \alpha'$．复合 $\theta=\psi\varphi^{-1}$ 是所要的同构． ■

定义 如果 K/k 是域扩张，$\alpha \in K$ 是 k 上的代数元素，则以 α 为根的唯一的首一不可约多项式 $p(x) \in k[x]$ 称为 k 上 α 的**极小多项式**，记为

$$\operatorname{irr}(\alpha, k)=p(x).$$

极小多项式 $\operatorname{irr}(\alpha,k)$ 依赖于 k. 例如，$\operatorname{irr}(i,\mathbb{R})=x^2+1$，而 $\operatorname{irr}(i, \mathbb{C})=x-i$.

下面的公式十分有用，特别是在对次数用归纳法证明一个定理的时候．

定理 3.121 设 $k \subseteq E \subseteq K$ 是域，且 E 是 k 的有限扩张，K 是 E 的有限扩张，则 K 是 k 的有限扩张，且

$$[K:k]=[K:E][E:k].$$

证明 如果 $A=a_1,\cdots,a_n$ 是 k 上的向量空间 E 的基，$B=b_1,\cdots,b_m$ 是 E 上的向量空间 K 的基，则只需证明由一切 a_ib_j 组成的表 X 是 k 上的向量空间 K 的基．

为证明 X 张成 K，取 $u \in K$．因 B 是 E 上 K 的基，存在标量 $\lambda_j \in E$ 使得 $u=\sum_j \lambda_j b_j$．因 A 是 k 上 E 的基，存在标量 $\mu_{ji} \in k$ 使得 $\lambda_j=\sum_i \mu_{ji} a_i$．所以 $u=\sum_{ij} \mu_{ji} a_i b_j$，从而 X 张成 k 上的 K.

为证明 X 在 k 上线性无关，假定存在标量 $\mu_{ji} \in k$ 使得 $\sum_{ij} \mu_{ji} a_i b_j=0$．如果定义 $\lambda_j=\sum_i \mu_{ji} a_i$，则 $\lambda_j \in E$ 且 $\sum_j \lambda_j b_j=0$．因 B 在 E 上线性无关，从而对一切 j，

$$0=\lambda_j=\sum_i \mu_{ji} a_i.$$

因 A 在 k 上线性无关，从而正如所要的，对一切 j 和 i，$\mu_{ji}=0$. ■

在欧几里得几何中有几个经典问题：三等分角；*倍立方*（给定边长为1的立方体，构造体积为2的立方体）；*圆求方*（给定半径为1的圆，构造一个正方形，其面积等于圆面积）．简单地说，这些问题是问这样的几何结构能否只用直尺和圆规按照确定的规则作出．定理3.121有一个漂亮的应用就是证明这些经典问题的不可解性．关于这些结果的讨论，读者可参考我的书《A First Course in Abstract Algebra》332～344页． 189

例3.122 设 $f(x)=x^4-10x^2+1\in\mathbb{Q}[x]$．如果 β 是 $f(x)$ 的根，则二次公式给出 $\beta^2=5\pm2\sqrt{6}$，而恒等式 $a+2\sqrt{ab}+b=(\sqrt{a}+\sqrt{b})^2$ 给出 $\beta=\pm(\sqrt{2}+\sqrt{3})$，同样，$5-2\sqrt{6}=(\sqrt{2}-\sqrt{3})^2$，所以 $f(x)$ 的根为

$$\sqrt{2}+\sqrt{3},-\sqrt{2}-\sqrt{3},\sqrt{2}-\sqrt{3},-\sqrt{2}+\sqrt{3}.$$

根据定理3.43，$f(x)$ 可能的有理根只有 ±1，从而正好证明了这些根都是无理的．

我们断言 $f(x)$ 在 $\mathbb{Q}[x]$ 中不可约．如果 $g(x)$ 是 $f(x)$ 在 $\mathbb{Q}[x]$ 中的二次因式，则

$$g(x)=(x-a\sqrt{2}-b\sqrt{3})(x-c\sqrt{2}-d\sqrt{3}),$$

其中 $a,b,c,d\in\{1,-1\}$．相乘得

$$g(x)=x^2-((a+c)\sqrt{2}+(b+d)\sqrt{3})x+2ac+3bd+(ad+bc)\sqrt{6}.$$

容易验证 $(a+c)\sqrt{2}+(b+d)\sqrt{3}$ 是有理的当且仅当 $a+c=0=b+d$，但这几个等式迫使 $ad+bc\neq0$，从而 $g(x)$ 的常数项不是有理的，因此 $g(x)\notin\mathbb{Q}[x]$，从而 $f(x)$ 在 $\mathbb{Q}[x]$ 中不可约．如果 $\beta=\sqrt{2}+\sqrt{3}$，则 $f(x)=\operatorname{irr}(\beta,\mathbb{Q})$．

考虑域 $E=\mathbb{Q}(\beta)=\mathbb{Q}(\sqrt{2}+\sqrt{3})$．存在域塔 $\mathbb{Q}\subseteq E\subseteq F$，其中 $F=\mathbb{Q}(\sqrt{2},\sqrt{3})$，从而由定理3.121，

$$[F:\mathbb{Q}]=[F:E][E:\mathbb{Q}].$$

因 $E=\mathbb{Q}(\beta)$ 且 β 是4次不可约多项式的根，也就是 $f(x)$ 的根，从而 $[E:\mathbb{Q}]=4$．另一方面，

$$[F:\mathbb{Q}]=[F:\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}].$$

因为 $\sqrt{2}$ 是 $\mathbb{Q}[x]$ 中二次不可约多项式 x^2-2 的根，$[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$．我们断言 $[F:\mathbb{Q}(\sqrt{2})]\leqslant2$．域 F 由添加 $\sqrt{3}$ 到 $\mathbb{Q}(\sqrt{2})$ 生成．不论 $\sqrt{3}\in\mathbb{Q}(\sqrt{2})$（此时次数是1），还是 x^2-3 在 $\mathbb{Q}(\sqrt{2})[x]$ 中不可约（此时次数是2）（事实上，次数是2）．由此 $[F:\mathbb{Q}]\leqslant4$，于是等式 $[F:\mathbb{Q}]=[F:E][E:\mathbb{Q}]$ 给出 $[F:E]=1$；即 $F=E$．

注意，$\mathbb{Q}$ 添加 $f(x)$ 的一切根产生 F，$\mathbb{Q}$ 添加 $g(x)=(x^2-2)(x^2-3)$ 的一切根也产生 F． ∎

现在证明两个重要结果：第一个属于克罗内克，说的是如果 $f(x)\in k[x]$，其中 k 是任意域，则存在包含 k 和 $f(x)$ 的所有根的某个更大的域 E；第二个属于伽罗瓦，构造了不同于 $\mathbb{F}_p$ 的有限域． 190

定理3.123（克罗内克） *如果 k 是域且 $f(x)\in k[x]$，则存在包含 k 并把它作为子域的域 K 使得 $f(x)$ 成为 $K[x]$ 中线性多项式的积．*

证明 对 $\deg(f)$ 用归纳法．如果 $\deg(f)=1$，则 $f(x)$ 是线性的，可以选取 $K=k$．如果 $\deg(f)>1$，记 $f(x)=p(x)g(x)$，其中 $p(x)$ 是不可约的．现在命题3.117(i)提供了一个包含 k 和 $p(x)$ 的一个根 z 的域 F．因此在 $F[x]$ 中有 $p(x)=(x-z)h(x)$ 和 $f(x)=(x-z)h(x)g(x)$．由归纳假设，存在域 K 包含 F（因此包含 k）使得 $h(x)g(x)$，从而 $f(x)$ 是 $K[x]$ 中线性因式的积． ∎

对于熟悉的域 $\mathbb{Q}$,$\mathbb{R}$ 和$\mathbb{C}$，克罗内克定理并没有提供新东西．代数基本定理于 1799 年首先由高斯证明（完成了欧拉和拉格朗日较早的尝试），定理表明每个非常数多项式 $f(x)\in\mathbb{C}[x]$ 在$\mathbb{C}$中都有一个根；从而可以对 $f(x)$ 的次数用归纳法，得到 $f(x)$ 的所有根都在$\mathbb{C}$中；即 $f(x)=a(x-r_1)\cdots(x-r_n)$，其中 $a\in\mathbb{C}$，且对一切 j. $r_j\in\mathbb{C}$. 另一方面，如果 $k=\mathbb{F}_p$ 或 $k=\mathbb{C}(x)=\mathrm{Frac}(\mathbb{C}[x])$，则基本定理用不上，而用克罗内克定理可以告诉我们，对于任意给定的 $f(x)$，恒存在一个更大的域 E 包含 $f(x)$ 的一切根．例如，存在某个域包含 $\mathbb{C}(x)$ 和 $\sqrt{x}$．第 6 章给出了基本定理的一个一般形式：每个域 k 都是一个**代数闭域**K 的子域，即 K 是包含 k 的域，使得每个 $f(x)\in K[x]$ 都是 $K[x]$ 中的线性多项式的积．相比之下，克罗内克定理一次只给出一个多项式的根．

$k(A)$ 是添加集合 A 到 k 得到的域，这个定义假定了 A 是 k 的域扩张 K 的子集．从克罗内克定理看来，我们可以说一个域扩张 $k(z_1,\cdots,z_n)$ 是添加某个 $f(x)\in k[x]$ 的一切根得到的，而不必怀疑这种扩张 K/k 是否存在．

定义 设 k 是域 K 的子域，且 $f(x)\in k[x]$．称 $f(x)$ 在 K 上**分裂**，如果

$$f(x)=a(x-z_1)\cdots(x-z_n),$$

其中 $z_1,\cdots,z_n$ 在 K 中，$a\in k$ 非零．

如果 $f(x)\in k[x]$ 是多项式，则域扩张 E/k 称为 $f(x)$ 在 k 上的一个**分裂域**，如果 $f(x)$ 在 E 上分裂，但 $f(x)$ 不在 E 的任一真子域上分裂．

例如考虑 $f(x)=x^2+1\in\mathbb{Q}[x]$．$f(x)$ 的根是$\pm\mathrm{i}$，从而 $f(x)$ 在$\mathbb{C}$上分裂；即 $f(x)=(x-\mathrm{i})(x+\mathrm{i})$ 是 $\mathbb{C}[x]$ 中线性多项式的积．但是$\mathbb{C}$不是$\mathbb{Q}$上的分裂域，因为$\mathbb{C}$不是包含$\mathbb{Q}$和 $f(x)$ 的一切根的最小域．$f(x)\in k[x]$ 的分裂域依赖于 $f(x)$，也依赖于 k：这里，$\mathbb{Q}$上的分裂域是 $\mathbb{Q}(\mathrm{i})$，$\mathbb{R}$上的分裂域是$\mathbb{R}(\mathrm{i})=\mathbb{C}$．

在例 3.122 中，我们证明了 $E=\mathbb{Q}(\sqrt{2}+\sqrt{3})$ 是 $f(x)=x^4-10x^2+1$ 的分裂域，也是 $g(x)=(x^2-2)(x^2-3)$ 的分裂域．

分裂域的存在性是克罗内克定理的简单推论．

191

系 3.124 设 k 是域，$f(x)\in k[x]$，则存在 $f(x)$ 在 k 上的分裂域．

证明 由克罗内克定理，存在域扩张 K/k 使得 $f(x)$ 在 $K[x]$ 中分裂，比如 $f(x)=a(x-\alpha_1)\cdots(x-\alpha_n)$. K 的子域 $E=k(\alpha_1,\cdots,\alpha_n)$ 是 $f(x)$ 在 k 上的分裂域． ■

这样，$f(x)\in k[x]$ 的一个分裂域是 K 的包含 k 和 $f(x)$ 的一切根的最小子域．我们说“一个”分裂域而不说“这个”分裂域的理由是分裂域的定义不只牵涉到 $f(x)$ 和 k，还牵涉到更大的域 K. 对于这个看法的深入分析可以使我们证明系 3.132：元素个数相等的任意两个有限域同构．

例 3.125 设 k 是域，并设 $E=k(y_1,\cdots,y_n)$ 是 k 上 n 个变量 $y_1,\cdots y_n$ 的有理函数域；即 n 元多项式的环的分式域 $E=\mathrm{Frac}(k[y_1,\cdots,y_n])$．$k$ 上 n **次一般多项式**定义为

$$f(x)=\prod_i(x-y_i)\in\mathrm{Frac}(k[y_1,\cdots,y_n])[x].$$

$f(x)=(x-y_1)(x-y_2)\cdots(x-y_n)$ 的系数记为 a_i，它可以用各 y 显式地给出[见198页等式(1)]. 注意 E 是 $f(x)$ 在域 $K=k(a_0,\cdots,a_{n-1})$ 上的分裂域，因为它由 K 添加 $f(x)$ 的一切根(就是一切 y)得到的. ■

下面是克罗内克定理的另一个应用．

命题 3.126 设 p 是素数，并设 k 是域．如果 $f(x)=x^p-c\in k[x]$ 且 α 是 c 的一个 p 次根（在

某个分裂域中），则或者 $f(x)$ 在 $k[x]$ 中不可约，或者 c 有一个 p 次根在 k 中．无论哪种情形，如果 k 包含 p 次单位根，则 $k(\alpha)$ 是 $f(x)$ 的一个分裂域．

证明　由克罗内克定理，存在包含 $f(x)$ 的一切根的域扩张 K/k，即 K 包含 c 的一切 p 次根．如果 $\alpha^p = c$，则 c 的每个 p 次根形为 $\omega\alpha$，其中 ω 是一个 p 次单位根，即 ω 是 $x^p - 1$ 的根．

如果 $f(x)$ 在 $k[x]$ 中不是不可约的，则在 $k[x]$ 中有因式分解 $f(x) = g(x)h(x)$，其中 $g(x)$ 是非常数多项式满足 $d = \deg(g) < \deg(f) = p$．现在 $g(x)$ 的常数项不计符号的话是 $f(x)$ 的一些根的乘积：

$$\pm b = \alpha^d \omega,$$

其中 ω 是 d 个 p 次单位根的乘积，它本身也是 p 次单位根．由此

$$(\pm b)^p = (\alpha^d \omega)^p = \alpha^{dq} = c^d.$$

但 p 是素数和 $d < p$ 迫使 $(d,p) = 1$，因此有整数 s 和 t 使得 $1 = sd + tp$．所以

$$c = c^{sd+tp} = c^{sd}c^{tp} = (\pm b)^{ps}c^{tp} = [(\pm b)^s c^t]^p.$$

192

因此 c 有 p 次根在 k 中．

如果 $\alpha \in K$ 是 c 的一个 p 次根，则 $f(x) = \prod_{\omega}(x - \omega\alpha)$，其中 ω 遍历 p 次单位根．因为现在假定所有 ω 在 k 中，从而 $k(\alpha)$ 是 $f(x)$ 的一个分裂域．■

由此，对每个素数 p，$x^p - 2$ 在 $\mathbb{Q}[x]$ 中不可约．

现在要构造有限域．我猜想伽罗瓦知道$\mathbb{C}$可以由添加多项式 x^2+1 的一个根到$\mathbb{R}$ 而构成，从而他自然会想到添加多项式的一个根到 $\mathbb{F}_p$．然而，我们注意到克罗内克定理直到伽罗瓦去世后半个世纪才得到证明．

定理 3.127（伽罗瓦）　*如果 p 是素数且 n 是正整数，则存在恰有 p^n 个元素的域．*

证明　记 $q = p^n$，考虑多项式

$$g(x) = x^q - x \in \mathbb{F}_p[x].$$

由克罗内克定理，存在包含 $\mathbb{F}_p$ 的域 K 使得 $g(x)$ 在 $K[x]$ 中是线性因式的乘积．定义

$$E = \{\alpha \in K : g(\alpha) = 0\};$$

于是 E 是 $g(x)$ 的一切根的集合．因导数 $g'(x) = qx^{q-1} - 1 = p^n x^{q-1} - 1 = -1$（见习题 3.23），从而 $\gcd(g, g')$ 是 1．由习题 3.37，$g(x)$ 的一切根都不同；即 E 恰有 $q = p^n$ 个元素．

我们断言 E 是 K 的子域，从而完成证明．如果 $a, b \in E$，则 $a^q = a, b^q = b$，所以 $(ab)^q = a^q b^q = ab$，因此 $ab \in E$．由习题 3.45，$(a-b)^q = a^q - b^q = a - b$，因此 $a - b \in E$．最后，如果 $a \neq 0$，则对 $a^q = a$ 运用消去律得 $a^{q-1} = 1$，从而 a 的逆是 a^{q-2}（因 E 在乘法下封闭，所以 a^{q-2} 在E 中）．■

我们立刻会看到元素个数相同的两个有限域同构．

回忆定理 3.30：有限域 k 的乘法群是循环群，这个群的生成元 α 叫做**本原元**；即 k 的每个非零元都是 α 的幂．

记号　*记有 $q = p^n$（其中 p 是素数）个元素的有限域为*

$$\mathbb{F}_q.$$

系 3.128　*对每个素数 p 和每个整数 $n \geq 1$，存在 n 次不可约多项式 $g(x) \in \mathbb{F}_p[x]$．事实上，如果 α 是 $\mathbb{F}_{p^n}$ 的本原元，则它的极小多项式 $g(x) = \mathrm{irr}(\alpha, \mathbb{F}_p)$ 的次数为 n.*

193

注　*对证明作简单修改，可以把$\mathbb{F}_p$ 换成任意有限域．*

证明　设域扩张 $E/\mathbb{F}_p$ 有 p^n 个元素，且 $\alpha \in E$ 是本原元．显然 $\mathbb{F}_p(\alpha) = E$，因为它包含 α 的每

个幂，从而包含 E 的每个非零元．由定理3.120(ⅰ)，$g(x)=\mathrm{irr}(\alpha,\mathbb{F}_p)\in\mathbb{F}_p[x]$ 是以 α 为根的不可约多项式．如果 $\deg(g)=d$，则命题3.117(ⅴ)给出 $[\mathbb{F}_p[x]/(g(x)):\mathbb{F}_p]=d$，但根据定理3.120(ⅰ)，$\mathbb{F}_p[x]/(g(x))\cong\mathbb{F}_p(\alpha)=E$，因此 $[E:\mathbb{F}_p]=n$．所以 $n=d$，从而 $g(x)$ 是 n 次不可约多项式． ■

这个系也可以用计数来证明．如果 $m=p_1^{e_1}\cdots p_n^{e_n}$，定义**默比乌斯函数**为

$$\mu(m)=\begin{cases}1 & \text{如果 } m=1\text{；}\\ 0 & \text{如果任一 } e_i>1\text{；}\\ (-1)^n & \text{如果 } 1=e_1=e_2=\cdots=e_n.\end{cases}$$

如果 N_n 是$\mathbb{F}_p[x]$中 n 次不可约多项式的个数，则

$$N_n=\frac{1}{n}\sum_{d\mid n}\mu(d)p^{n/d}.$$

一个初等证明可在 G. J. Simmons, "The Number of Irreducible Polynomials of Degree n over GF(p)," *American Mathematical Monthly* 77 (1970)，743～745 页中找到．

例 3.129 (ⅰ) 在习题 3.14 中，构造了有四个元素的域 k：

$$k=\left\{\begin{bmatrix}a & b\\ b & a+b\end{bmatrix}: a,b\in\mathbb{I}_2\right\}.$$

另一方面，可以构造作为商域 $F=\mathbb{F}_2[x]/(q(x))$ 的 4 阶域，其中 $q(x)\in\mathbb{F}_2[x]$ 是不可约多项式 x^2+x+1．根据命题3.117(ⅴ)，F 是由一切 $a+bz$ 组成的域，其中 $z=x+(q(x))$ 是 $q(x)$ 的根且 $a,b\in\mathbb{I}_2$．因 $z^2+z+1=0$，有 $z^2=-z-1=z+1$，此外，$z^3=zz^2=z(z+1)=z^2+z=1$．现在易知存在环同态 $\varphi:k\to F$ 使得

$$\varphi\left(\begin{bmatrix}a & b\\ b & a+b\end{bmatrix}\right)=a+bz.$$

(ⅱ) 按照例3.35(ⅱ)中的表，在 $\mathbb{F}_3[x]$ 中有三个首一不可约二次多项式，就是

$$p(x)=x^2+1,q(x)=x^2+x-1 \text{ 和 } r(x)=x^2-x-1,$$

每个形成有 $9=3^2$ 个元素的域．我们更详细地考察头两个域．命题3.117(ⅴ)表明 $E=\mathbb{F}_3[x]/(p(x))$ 由

194

$$E=\{a+b\alpha:\text{其中 } \alpha^2+1=0\}$$

给出．同样，如果 $F=\mathbb{F}_3[x]/(q(x))$，则

$$F=\{a+b\beta:\text{其中 } \beta^2+\beta-1=0\}.$$

因为由

$$\varphi(a+b\alpha)=a+b(1-\beta)$$

定义的映射 $\varphi:E\to F$（用尝试法找到）是同构，所以这两个域是同构的．

现在$\mathbb{F}_3[x]/(x^2-x-1)$ 也是有 9 个元素的域，可以证明它同构于刚才给出的两个域 E 和 F（见系 3.132）．

(ⅲ) 在例3.35(ⅱ)中，展示了 8 个首一不可约三次多项式 $p(x)\in\mathbb{F}_3[x]$，每个形成有 $27=3^3$ 个元素的域 $\mathbb{F}_3[x]/(p(x))$． ■

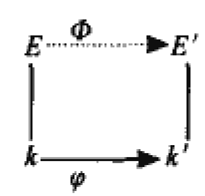
现在来解决有限域的同构问题．

引理 3.130 设 $f(x)\in k[x]$，其中 k 是域，并设 E 是 $f(x)$ 在 k 上的分裂域．设 $\varphi:k\to k'$ 是

一个域同构，设 $\varphi^*: k[x] \to k'[x]$ 是由

$$g(x) = a_0 + a_1 x + \cdots + a_n x^n \mapsto g^*(x) = \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n$$

给出的同构，并设 E' 是 $f^*(x)$ 在 k' 上的分裂域，则存在同构 $\Phi: E \to E'$，且是 φ 的扩张．



证明 对 $d = [E:k]$ 用归纳法证明．如果 $d = 1$，则 $f(x)$ 是 $k[x]$ 中的线性多项式的乘积，由此易知 $f^*(x)$ 也是 $k'[x]$ 中的线性多项式的乘积．所以 $E' = k'$，且可令 $\Phi = \varphi$.

关于归纳步，选取 $f(x)$ 在 E 中但不在 k 中的一个根 z，令 $p(x) = \mathrm{irr}(z,k)$ 为 z 在 k 上的最小多项式（命题 3.117）．现在因为 $z \notin k$，所以 $\deg(p) > 1$．此外，根据命题 3.117，$[k(z):k] = \deg(p)$．设 z' 是 $f^*(x)$ 在 E' 中的根，且 $p^*(x) = \mathrm{irr}(z',k')$ 为 $k'[x]$ 中相应的首一不可约多项式．

根据命题 3.120（ii）的一个直接推广[⊖]，存在扩张 φ 的同构 $\tilde{\varphi}: k(z) \to k'(z')$ 满足 $\tilde{\varphi}: z \mapsto z'$．可以把 $f(x)$ 看成系数在 $k(z)$ 中的多项式（因为 $k \subseteq k(z)$ 蕴涵 $k[x] \subseteq k(z)[x]$）．我们断言 E 是 $f(x)$ 在 $k(z)$ 上的分裂域；即 [195]

$$E = k(z)(z_1, \cdots, z_n),$$

其中 $z_1, \cdots, z_n$ 是 $f(x)/(x-z)$ 的根，毕竟

$$E = k(z, z_1, \cdots, z_n) = k(z)(z_1, \cdots, z_n).$$

类似地，E' 是 $f^*(x)$ 在 $k'(z')$ 上的分裂域．但根据定理 3.121，$[E:k(z)] < [E:k]$，从而归纳假设给出同构 $\Phi: E \to E'$，它是 $\tilde{\varphi}$ 的扩张，因此也是 φ 的扩张． ■

定理 3.131 *如果 k 是域且 $f(x) \in k[x]$，则 $f(x)$ 在 k 上的任意两个分裂域通过一个逐点固定 k 的同构映射而同构．*

证明 设 E 和 E' 是 $f(x)$ 在 k 上的分裂域．如果 φ 为恒等函数，则定理立即成立． ■

值得注意的是直到 19 世纪 90 年代，即伽罗瓦发现有限群之后的 60 年后下一定理才得到证明．

系 3.132（穆尔） *恰有 p^n 个元素的任何两个有限域同构．*

证明 如果 E 是有 $q = p^n$ 个元素的域，则把拉格朗日定理应用到乘法群 $E^\times$ 上证明对每个 $a \in E^\times$ 有 $a^{q-1} = 1$．从而 E 的每个元素是 $f(x) = x^q - x \in \mathbb{F}_p[x]$ 的根，于是 E 是 $f(x)$ 在 $\mathbb{F}_p$ 上的分裂域． ■

穆尔（E. H. Moore，1862—1932）作为一个代数学家开始他的数学生涯，但他也在数学的其他许多领域做出重要工作，例如穆尔-史密斯收敛，一半以他的名字命名．

常称有限域为伽罗瓦域以纪念它的发现者．从系 3.132 看来，我们可以说有 q 个元素的域，其中 $q = p^n$ 是素数 p 的幂．

习题

3.81 证明：如果 $I = \{0\}$，则 $R/I \cong R$．

⊖ 较早证明这个推广会涉及现在假设中的一切记号的引入，从而会把一个简单结果变得复杂．同构 $\varphi: k \to k'$ 导出同构 $\varphi^*: k[x] \to k'[x]$，$\varphi^*$ 把 $p(x)$ 变为某个多项式 $p^*(x)$，而 φ^* 又导出同构 $k[x]/(p(x)) \to k'[x]/(p^*(x))$．

3.82 **（环的第三同构定理）** 如果 R 是有理想 $I \subseteq J$ 的交换环，则 J/I 是 R/I 中的理想，且存在环同构 $(R/I)/(J/I) \cong R/J$.

3.83 对每个交换环 R，证明 $R[x]/(x) \cong R$.

196 3.84 证明 $\mathbb{F}_3[x]/(x^3 - x^2 + 1) \cong \mathbb{F}_3[x]/(x^3 - x^2 + x + 1)$.

3.85 如果 X 是交换环 R 的子集，定义 $\mathcal{I}(X)$ 为 R 中一切包含 X 的理想 I 的交．证明 $\mathcal{I}(X)$ 是所有这样的 $a \in R$ 组成的集合，对于 a 存在有限多个元素 $x_1, \cdots, x_n \in X$ 和 $r_i \in R$ 使得 $a = r_1x_1 + \cdots + r_nx_n$.

3.86 设 $h(x), p(x) \in k[x]$ 是首一多项式，其中 k 是域．如果 $p(x)$ 是不可约的，且 $h(x)$ 的每个根（在适当的分裂域中）也是 $p(x)$ 的根，证明有某个整数 $m \geqslant 1$ 使得 $h(x) = p(x)^m$.

提示：对 $\deg(h)$ 用归纳法．

3.87 **孙子剩余定理**．

（ⅰ）如果 k 是域且 $f(x), f'(x) \in k[x]$ 互素，证明给定 $b(x), b'(x) \in k[x]$，存在 $c(x) \in k[x]$ 使得

$$c - b \in (f) \text{ 和 } c - b' \in (f').$$

此外，如果 $d(x)$ 是另一个公共解，则 $c - d \in (ff')$.

提示：采用定理 1.28 的证明．本习题在习题6.11(ⅲ)中推广到交换环上．

（ⅱ）如果 k 是域且 $f(x), g(x) \in k[x]$ 互素，证明

$$k[x]/(f(x)g(x)) \cong k[x]/(f(x)) \times k[x]/(g(x)).$$

提示：见定理 2.81 的证明．

3.88 （ⅰ）证明一个域 K 不可能有子域 k' 和 k'' 满足 $k' \cong \mathbb{Q}$ 且 $k'' \cong \mathbb{F}_p$，其中 p 是某个素数．

（ⅱ）证明一个域 K 不可能有子域 k' 和 k'' 满足 $k' \cong \mathbb{F}_p$ 且 $k'' \cong \mathbb{F}_q$，其中 $p \neq q$ 是素数．

3.89 证明随机群 $\Sigma(2, \mathbb{F}_4) \cong A_4$.

提示：见习题 3.19.

3.90 设 $f(x) = s_0 + s_1x + \cdots + s_{n-1}x^{n-1} + x^n \in k[x]$，其中 k 是域，并假设 $f(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)$. 证明 $s_{n-1} = -(\alpha_1 + \alpha_2 + \cdots + \alpha_n)$ 和 $s_0 = (-1)^n\alpha_1\alpha_2\cdots\alpha_n$. 由此可知 $f(x)$ 的一切根的和与积都在 k 中．

3.91 写出有 8 个元素的域 $\mathbb{F}_8$ 的加法和乘法表．

提示：用 $\mathbb{F}_2$ 上的一个不可约三次多项式．

3.92 设 $k \subseteq K \subseteq E$ 是域．证明：如果 E 是 k 的有限扩张，则 E 是 K 的有限扩张且 K 是 k 的有限扩张．

提示：用系3.90(ⅱ).

3.93 设 $k \subseteq F \subseteq K$ 是域塔，且 $z \in K$. 证明：如果 $k(z)/k$ 有限，则 $[F(z):F] \leqslant [k(z):k]$，特别地，$[F(z):F]$ 有限．

提示：用命题 3.117 获得一个不可约多项式 $p(x) \in k[x]$，该多项式 $p(x)$ 在 $K[x]$ 中可分解．

3.94 （ⅰ）$\mathbb{F}_4$ 是 $\mathbb{F}_8$ 的子域吗？

（ⅱ）对每个素数 p 证明：如果 $\mathbb{F}_{p^n}$ 是 $\mathbb{F}_{p^m}$ 的子域，则 $n \mid m$（后面我们将看到逆命题也成立）．

提示：把 $\mathbb{F}_{p^m}$ 看作 $\mathbb{F}_{p^n}$ 上的向量空间．

197 3.95 设 K/k 是域扩张．如果 $A \subseteq K$ 和 $u \in k(A)$，证明存在 $a_1, \cdots, a_n \in A$ 使得 $u \in k(a_1, \cdots, a_n)$.

第4章 域

4.1 五次方程的不可解性

本章讨论当今所说的伽罗瓦理论（原先称为方程论），即域扩张与那些和它相关的叫做伽罗瓦群之间的相互关系. 这一理论使我们能够证明阿贝尔-鲁菲尼定理和伽罗瓦定理，它们精确地描述了什么时候二次多项式的求根公式可以推广到高次多项式. 这一理论的另一推论是给出了代数基本定理的一个证明.

根据定理 3.123，即克罗内克定理，对每个首一多项式 $f(x) \in k[x]$，其中 k 是域，存在包含 k 和（不必不同）根 $z_1, \cdots, z_n$ 的域 K 使得

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = (x - z_1)\cdots(x - z_n).$$

对 $n \geqslant 1$ 用归纳法，可以容易地推广[㊀] 习题 3.90：

$$\begin{cases} a_{n-1} = -\sum_i z_i \\ a_{n-2} = \sum_{i<j} z_i z_j \\ a_{n-3} = -\sum_{i<j<k} z_i z_j z_k \\ \quad\vdots \\ a_0 = (-1)^n z_1 z_2 \cdots z_n. \end{cases} \tag{1}$$

198

注意 $-a_{n-1}$ 是根的和，$\pm a_0$ 是根的积. 给定 $f(x)$ 的系数，能否求出它的根；即给定各个 a，能否解有 n 个未知数和 n 个方程的方程组 (1)? 如果 $n=2$，答案是肯定的：二次公式就可以解. 如果 $n=3$ 或 4，答案仍然是肯定的，因为三次和四次公式可以解. 但 $n \geqslant 5$，我们将看到不存在类似的解.

我们不是说当 $n \geqslant 5$ 时方程组 (1) 无解，而是说不存在类似经典公式那样的解. 如果不限制自己仅用域的运算和开方，那么很可能存在某种方法求五次多项式的根. 事实上，可以用牛顿法求根：如果 r 是多项式 $f(x)$ 的一个实根，而 x_0 是 r 的一个"好"的近似，则 $r = \lim_{n\to\infty} x_n$，其中 x_n 递推地定义为对一切 $n \geqslant 0, x_{n+1} = x_n - f(x_n)/f'(x_n)$. 还有埃尔米特的方法，用椭圆模函数求五次方程的根，还有用超几何函数求许多高次多项式根的方法.

我们要证明当 $n \geqslant 5$ 时没有"根式"解（后面要仔细定义这个概念）. 考察的关键是出现对称. 回忆第 2 章，如果 Ω 是平面 $\mathbb{R}^2$ 上的多边形，则它的对称群 $\Sigma(\Omega)$ 由满足 $\varphi(\Omega) = \Omega$ 的平面运动 $\varphi: \mathbb{R}^2 \to \mathbb{R}^2$ 组成. 此外，运动 $\varphi \in \Sigma(\Omega)$ 被 Ω 顶点的值完全确定，事实上，如果 Ω 有 n 个顶点，则 $\Sigma(\Omega)$ 同构于 S_n 的一个子群.

我们要设置对称群的一个类似，在那里多项式扮演了多边形的角色，多项式的分裂域扮演了平

㊀ 系数 a_i 可以看作 $z_1, \cdots, z_n$ 中的多项式，此时称它们为**初等对称多项式**，因为它们不随那些 z 的排列而改变.

面$\mathbb{R}^2$的角色，固定k的自同构扮演了运动的角色.

定义 设E是包含子域k的域. 称同构$\sigma: E \to E$为E的**自同构**[⊖]；称σ**固定**k如果对每个$a \in k, \sigma(a) = a$.

例如考虑$f(x) = x^2 + 1 \in \mathbb{Q}[x]$. $f(x)$在$\mathbb{Q}$上的一个分裂域是$E = \mathbb{Q}(\mathrm{i})$，复共轭$\sigma: \alpha \mapsto \bar{\alpha}$是$E$的固定$\mathbb{Q}$的自同构的一个例子.

命题 4.1 设k是域K的子域，设

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in k[x],$$

并设$E = k(z_1, \cdots, z_n) \subseteq K$是一个分裂域. 如果$\sigma: E \to E$是固定$k$的自同构，则$\sigma$置换$f(x)$的根$\{z_1, \cdots, z_n\}$的集合.

证明 如果r是$f(x)$的根，则

199

$$0 = f(r) = r^n + a_{n-1}r^{n-1} + \cdots + a_1 r + a_0.$$

把σ作用到这个等式上，因σ固定k，得

$$\begin{aligned} 0 &= \sigma(r)^n + \sigma(a_{n-1})\sigma(r)^{n-1} + \cdots + \sigma(a_1)\sigma(r) + \sigma(a_0) \\ &= \sigma(r)^n + a_{n-1}\sigma(r)^{n-1} + \cdots + a_1\sigma(r) + a_0 \\ &= f(\sigma(r)), \end{aligned}$$

所以$\sigma(r)$是$f(x)$的根. 如果Z是一切根的集合，则$\sigma | Z: Z \to Z$，其中$\sigma | Z$是σ的限制. 但$\sigma | Z$是单射（因σ是单射），从而由习题 1.58，$\sigma | Z$是Z的置换. ■

下面是多边形Ω的对称群$\Sigma(\Omega)$的类似.

定义 设k是域E的子域. E在k上的**伽罗瓦群**是指E的固定k的一切自同构的集合，记为$\mathrm{Gal}(E/k)$. 如果$f(x) \in k[x]$，且$E = k(z_1, \cdots, z_n)$是一个分裂域，则定义$f(x)$在k上的**伽罗瓦群**为$\mathrm{Gal}(E/k)$.

容易验证$\mathrm{Gal}(E/k)$是以函数复合作为运算的群. 该定义属于阿廷（E. Artin，1898—1962），保持了他和诺特（E. Noether）强调"抽象"代数的风格，伽罗瓦的原始定义（群同构于这里定义的群）其措辞不是自同构，而是多项式根的某种置换（见 Tignol 所著的《Galois' Theory of Algebraic Equations》306～331 页）. 注意，由定理 3.131，$\mathrm{Gal}(E/k)$不依赖于分裂域E的选取.

下面的引理将一再用到.

引理 4.2 设$E = k(z_1, \cdots, z_n)$. 如果$\sigma: E \to E$是固定k的自同构，即$\sigma \in \mathrm{Gal}(E/k)$，且对于一切$i, \sigma(z_i) = z_i$，则$\sigma$是恒等函数$1_E$.

证明 对$n \geqslant 1$用归纳法证明该引理. 如果$n=1$，则每个$u \in E$形如$u = f(z_1)/g(z_1)$，其中$f(x), g(x) \in k[x]$，且$g(z_1) \neq 0$. 但σ固定z_1以及$f(x)$和$g(x)$的系数，从而σ固定一切$u \in E$. 关于归纳步，记$K = k(z_1, \cdots, z_{n-1})$并注意到$E = K(z_n)$[因为$K(z_n)$是包含$k$和$z_1, \cdots, z_{n-1}, z_n$的最小域]. 只要在基础步的论证中把$k$换成$K$，就完成了归纳步的论证. ■

定理 4.3 如果$f(x) \in k[x]$次数为n，则它的伽罗瓦群$\mathrm{Gal}(E/k)$同构于S_n的一个子群.

证明 设$X = \{z_1, \cdots, z_n\}$. 如果$\sigma \in \mathrm{Gal}(E/k)$，则命题 4.1 证明它的限制$\sigma | X$是$X$的一个置换；即$\sigma | X \in S_X$. 定义$\varphi: \mathrm{Gal}(E/k) \to S_X$为$\varphi: \sigma \mapsto \sigma | X$. 为证明$\varphi$是同构，注意$\varphi(\sigma\tau)$和$\varphi(\sigma)\varphi(\tau)$两者都是函数$X \to X$，因此只要它们在每个$z_i \in X$上一致就相等. 但$\varphi(\sigma\tau): z_i \mapsto (\sigma\tau)(z_i)$，而$\varphi(\sigma)\varphi(\tau): z_i \mapsto$

⊖ 字 automorphism（自同构）由两个希腊字根组成，意为"自己"的 auto 和意为"形状"或"形式"的 morph. 如同同构把一个群带到一个等同的复制群上，自同构把一个群带到它自己上面.

$\sigma(\tau(z_i))$，它们是相同的.

φ 的象是 $S_X \cong S_n$ 的子群. φ 的核是在 X 上形成恒等置换 $\sigma \in \mathrm{Gal}(E/k)$ 的集合；即 σ 固定每个根 z_i. 根据伽罗瓦群的定义，σ 也固定 k，引理 4.2 给出 $\ker\varphi = \{1\}$. 所以 φ 是单射，定理得证. ■ [200]

如果 $f(x) = x^2 + 1 \in \mathbb{Q}[x]$，则复共轭 σ 是它的分裂域$\mathbb{Q}(i)$ 的自同构，它固定$\mathbb{Q}$（交换根 i 和 $-i$）. 因 $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$ 是对称群 S_2 的子群，S_2 的阶为 2，从而 $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \langle\sigma\rangle \cong \mathbb{I}_2$. 可以把任一伽罗瓦群的元素看作复共轭的推广.

我们要计算伽罗瓦群的阶，但先要获得关于域同构和自同构的一些信息.

引理 4.4 *如果 k 是特征为 0 的域，则每个不可约多项式 $p(x) \in k[x]$ 都没有重根.*

证明 在习题 3.37 中看到，系数在任意域中的任意（不必不可约）多项式 $f(x)$ 无重根当且仅当 $\gcd(f, f') = 1$，其中 $f'(x)$ 是 $f(x)$ 的导数.

现在考虑 $p(x) \in k[x]$. 不是 $p'(x) = 0$ 就是 $\deg(p') < \deg(p)$. 因 $p(x)$ 是不可约的，它不是常数，从而它有某个非零单项式 $a_i x^i$，其中 $i \geqslant 1$. 因 k 有特征 0，所以 $i a_i x^{i-1}$ 是 $p'(x)$ 中的非零单项式，从而 $p'(x) \neq 0$. 最后，因 $p(x)$ 是不可约的，它的因式只有常数和相伴多项式，由于 $p'(x)$ 的次数较小，因而它不可能是 $p(x)$ 的相伴多项式，所以 $\gcd(p', p) = 1$. ■

回忆定理3.120（i）：如果 E/k 是一个扩张，且 $\alpha \in E$ 是 k 上的代数数，则存在唯一的首一不可约多项式 $\mathrm{irr}(\alpha, k) \in k[x]$ 以 α 为根，这个多项式叫做 α 的*极小多项式*.

定义 *设 E/k 是一个代数扩张. 如果不可约多项式 $p(x)$ 没有重根，则称 $p(x)$ 是***可分***的. 对一个任意多项式 $f(x)$，如果它的每个不可约因式无重根，则称 $f(x)$ 是***可分***的.*

*元素 $\alpha \in E$ 称为***可分***的，如果 α 或者是 k 上的超越元数，或者是 k 上的代数元素，而它的极小多项式 $\mathrm{irr}(\alpha, k)$ 无重根；即 $\mathrm{irr}(\alpha, k)$ 是可分多项式.*

*域扩张 E/k 称为***可分扩张***，如果它的每个元素都是可分的；称 E/k 为***不可分***的，如果它不是可分的.*

引理 4.4 表明特征 0 的域的每个扩张都是可分扩张. 如果 E 是有 p^n 个元素的有限域，则拉格朗日定理（对乘法群 $E^\times$）表明 E 的每个元素都是 $x^{p^n} - x$ 的根. 在定理 3.127（有 p^n 个元素的有限域的存在性）的证明中看到，$x^{p^n} - x$ 无重根. 由此，如果 $k \subseteq E$，则因对 $\alpha \in E$，$\mathrm{irr}(\alpha, k)$ 是$x^{p^n} - x$ 的因式，从而 E/k 是可分扩张.

例 4.5 这是一个不可分扩张的例子. 设 $k = \mathbb{F}_p(t) = \mathrm{Frac}(\mathbb{F}_p[t])$，并设 $E = k(\alpha)$，其中 α 是 $f(x) = x^p - t$ 的根；即 $\alpha^p = t$. 在 $E[x]$ 中，有

$$f(x) = x^p - t = x^p - \alpha^p = (x - \alpha)^p.$$

[201]

如果证明了 $\alpha \notin k$，则由命题 3.126，$f(x)$ 是不可约的，从而 $f(x) = \mathrm{irr}(\alpha, k)$ 是不可分多项式. 所以 E/k 是不可分扩张.

剩下的是证明 $\alpha \notin k$. 如果不是这样，则存在 $g(t), h(t) \in \mathbb{F}_p[t]$ 使得 $\alpha = g(t)/h(t)$，因此 $g = \alpha h$ 且 $g^p = \alpha^p h^p = t h^p$，从而

$$\deg(g^p) = \deg(t h^p) = 1 + \deg(h^p).$$

但 $p \mid \deg(g^p)$ 且 $p \mid \deg(h^p)$，这就得出矛盾. ■

第 6 章中我们将更彻底地研究可分性和不可分性.

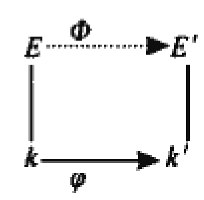
例 4.6 设 m 是正整数，k 是域，并设 $f(x) = x^m - 1 \in k[x]$. 如果 k 的特征不整除 m，则$mx^{m-1} \neq 0$

且 $\gcd(f,f')=1$,因此 $f(x)$ 没有重根. 所以 $f(x)$ 的任意一个分裂域 E/k 包含 m 个不同的 m 次单位根. 此外,这些单位根的集合是 $E^{\times}$ 的 m 阶(乘法)子群,且由定理 3.30,它是循环群. 我们已经证明如果域 k 的特征不整除 m,则在 k 的某个扩域中存在 m 次单位原根 ω,且 ω 是可分元素.

另一方面,如果 p^e 是素数幂且 k 有特征 p,则 $x^{p^e}-1=(x-1)^{p^e}$,从而只有一个 p^e 次单位根,就是 1. ■

E/k 的可分性使我们能够求 $\mathrm{Gal}(E/k)$ 的阶.

定理 4.7 (i) 设 E/k 是可分多项式 $f(x)\in k[x]$ 的分裂域,$\varphi:k\to k'$ 是域同构,且 E'/k' 是 $f^*(x)\in k'[x]$ 的分裂域 [其中 $f^*(x)$ 是把 φ 作用到 $f(x)$ 的系数上得到的].



则恰有 $[E:k]$ 个扩张 φ 的同构 $\Phi:E\to E'$.

(ii) 如果 E/k 是可分 $f(x)\in k[x]$ 的一个分裂域,则

$$|\mathrm{Gal}(E/k)|=[E:k].$$

证明 (i) 对 $[E:k]$ 用归纳法的这个证明是引理 3.130 的修改. 如果 $[E:k]=1$,则 $E=k$ 且只有一个 φ 的扩张 Φ,就是 φ 自己. 如果 $[E:k]>1$,令 $f(x)=p(x)g(x)$,其中 $p(x)$ 是最高次数的不可约因式,比如 d 次不可约因式. 可以假定 $d>1$,否则 $f(x)$ 在 k 上分裂,从而 $[E:k]=1$. 选取 $p(x)$ 的一个根 α(注意,因为 E 是 $f(x)=p(x)g(x)$ 的分裂域,所以 $\alpha\in E$). 如果 $\widetilde{\varphi}:k(\alpha)\to E'$ 是 φ 的任一扩张,则由命题 4.1,$\varphi(\alpha)$ 是 $p^*(x)$ 的根 α'. 因 $f^*(x)$ 是可分的,$p^*(x)$ 恰有 d 个根 $\alpha'\in E'$. 由引理 4.2 和定理 3.12 (ii),恰有 d 个扩张 φ 的同构 $\hat{\varphi}:k(\alpha)\to k'(\alpha')$,每个 α' 有一个. 现在 E 也是 $f(x)$ 在 $k(\alpha)$ 上的分裂域,这是因为添加 $f(x)$ 的一切根到 $k(\alpha)$ 仍然产生 E,且 E' 是 $f^*(x)$ 在 $k'(\alpha')$ 上的分裂域. 因 $[E:k(\alpha)]=[E:k]/d$,归纳假设表明 d 个同构 $\hat{\varphi}$ 的每一个恰有 $[E:k]/d$ 个扩张 $\Phi:E\to E'$. 由此我们已经构造了 $[E:k]$ 个扩张 φ 的同构. 因为对于每个扩张 φ 的 τ 都有某个 $\hat{\varphi}:k(\alpha)\to k'(\alpha')$ 使得 $\tau\mid k(\alpha)=\hat{\varphi}$,所以再没有其他的同构.

(ii) 在 (i) 中取 $k=k'$,$E=E'$ 和 $\varphi=1_k$. ■

例 4.8 在定理 4.7 (ii) 中,可分性的假设是必要的. 在例 4.5 中看到,如果 $k=\mathbb{F}_p(t)$ 且 α 是 x^p-t 的一个根,则 $E=k(\alpha)$ 是一个不可分扩张. 此外,$x^p-t=(x-\alpha)^p$,从而 α 是这个多项式的唯一的根. 因此,如果 $\sigma\in\mathrm{Gal}(E/k)$,则命题 4.1 表明 $\sigma(\alpha)=\alpha$. 因此由引理 4.2,$\mathrm{Gal}(E/k)=\{1\}$,从而此时 $|\mathrm{Gal}(E/k)|<[E:k]=p$. ■

系 4.9 设 E/k 是 n 次可分多项式 $f(x)\in k[x]$ 的一个分裂域. 如果 $f(x)$ 是不可约的,则 $n\mid|\mathrm{Gal}(E/k)|$.

证明 由定理,$|\mathrm{Gal}(E/k)|=[E:k]$. 令 $\alpha\in E$ 是 $f(x)$ 的一个根,因 $f(x)$ 是不可约的,所以 $[k(\alpha):k]=n$,且

$$[E:k]=[E:k(\alpha)][k(\alpha):k]=n[E:k(\alpha)].$$ ■

在命题 4.38 中我们将看到,如果 E/k 是可分多项式的分裂域,则 E/k 是可分扩张.

下面计算 $\mathbb{Q}[x]$ 中几个特殊多项式的伽罗瓦群.

例 4.10 （ⅰ）设 $f(x)=x^3-1\in\mathbb{Q}[x]$. 现在 $f(x)=(x-1)(x^2+x+1)$，其中 x^2+x+1 是不可约的（二次公式表明它的根 ω 和 $\overline{\omega}$ 不在$\mathbb{Q}$中）. $f(x)$ 的分裂域是 $\mathbb{Q}(\omega)$，因 $\omega^2=\overline{\omega}$，从而 $[\mathbb{Q}(\omega):\mathbb{Q}]=2$. 所以根据定理 4.7（ⅱ），$|\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})|=2$，它是 2 阶循环群，它的非平凡元素是复共轭.

（ⅱ）设 $f(x)=x^2-2\in\mathbb{Q}[x]$. 现在 $f(x)$ 是不可约的，根为$\pm\sqrt{2}$，从而 $E=\mathbb{Q}(\sqrt{2})$ 是分裂域. 根据定理4.7（ⅱ），$|\mathrm{Gal}(E/\mathbb{Q})|=2$. 现在 E 的每个元素有形如 $a+b\sqrt{2}$的唯一表达式，其中 a，$b\in\mathbb{Q}$[定理 3.117（ⅴ）]，易知由 $\sigma: a+b\sqrt{2}\mapsto a-b\sqrt{2}$ 定义的 $\sigma: E\to E$ 是 E 的固定$\mathbb{Q}$的自同构，所以 $\mathrm{Gal}(E/\mathbb{Q})=\langle\sigma\rangle$，其中 σ 交换$\sqrt{2}$和$-\sqrt{2}$.

（ⅲ）设 $g(x)=x^3-2\in\mathbb{Q}[x]$. $g(x)$ 的根是 $\alpha,\omega\alpha,\omega^2\alpha$，其中 $\alpha=\sqrt[3]{2}$，它是 2 的实立方根，ω 是三次单位原根. 易知 $g(x)$ 的分裂域是 $E=\mathbb{Q}(\alpha,\omega)$. 因为 $g(x)$ 在$\mathbb{Q}$上不可约（它是没有有理根的三次多项式），因此

$$[E:\mathbb{Q}]=[E:\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}]=3[E:\mathbb{Q}(\alpha)],$$

203

现在因为 $\mathbb{Q}(\alpha)$ 中的元素都是实数，而复数 ω 不是实数，从而 $E\neq\mathbb{Q}(\alpha)$. 所以 $[E:\mathbb{Q}]=|\mathrm{Gal}(E/\mathbb{Q})|>3$. 另一方面，我们知道 $\mathrm{Gal}(E/\mathbb{Q})$ 同构于 S_3 的一个子群，因此必有 $\mathrm{Gal}(E/\mathbb{Q})\cong S_3$.

（ⅳ）在例 3.122 中考察过 $f(x)=x^4-10x^2+1\in\mathbb{Q}[x]$，可知 $f(x)$ 是不可约的. 事实上，$f(x)=\mathrm{irr}(\beta,\mathbb{Q})$，其中 $\beta=\sqrt{2}+\sqrt{3}$. 如果 $E=\mathbb{Q}(\beta)$，则$[E:\mathbb{Q}]=4$. 此外，E 是 $f(x)$ 的分裂域，其中 $f(x)$ 的另外三个根是 $-\sqrt{2}-\sqrt{3}$，$-\sqrt{2}+\sqrt{3}$，$\sqrt{2}-\sqrt{3}$. 由定理4.7（ⅱ），如果 $G=\mathrm{Gal}(E/\mathbb{Q})$，则 $|G|=4$. 因此 $G\cong\mathbb{I}_4$ 或 $G\cong\mathbf{V}$.

在例 3.122 中还看到，E 包含$\sqrt{2}$和$\sqrt{3}$. 如果 σ 是 E 的固定$\mathbb{Q}$的自同构，因为 $(\sigma(\sqrt{2}))^2=2$，从而 $\sigma(\sqrt{2})=u\sqrt{2}$，其中 $u=\pm1$. 所以 $\sigma^2(\sqrt{2})=\sigma(u\sqrt{2})=u\sigma(\sqrt{2})=u^2\sqrt{2}=\sqrt{2}$；同样，$\sigma^2(\sqrt{3})=\sqrt{3}$. 如果 α 是 $f(x)$ 的一个根，则 $\alpha=u\sqrt{2}+v\sqrt{3}$，其中 $u,v=\pm1$，因此，

$$\sigma^2(\alpha)=u\sigma^2(\sqrt{2})+v\sigma^2(\sqrt{3})=u\sqrt{2}+v\sqrt{3}=\alpha.$$

引理 4.2 给出对一切 $\sigma\in\mathrm{Gal}(E/\mathbb{Q})$，$\sigma^2=1_E$，从而 $\mathrm{Gal}(E/\mathbb{Q})\cong\mathbf{V}$.

还有另一种方法计算 $G=\mathrm{Gal}(E/\mathbb{Q})$. 在例 3.122 中我们看到 $E=\mathbb{Q}(\sqrt{2}+\sqrt{3})=\mathbb{Q}(\sqrt{2},\sqrt{3})$ 也是 $g(x)=(x^2-2)(x^2-3)$ 在$\mathbb{Q}$上的分裂域. 由命题 3.120（ⅱ），存在自同构 $\varphi:\mathbb{Q}(\sqrt{2})\to\mathbb{Q}(\sqrt{2})$ 把 $\sqrt{2}\mapsto-\sqrt{2}$. 如同我们在例 3.122 中注意到的，$\sqrt{3}\notin\mathbb{Q}(\sqrt{2})$，从而 x^2-3 在$\mathbb{Q}(\sqrt{2})$上不可约. 引理 3.130 证明 φ 可以扩张为自同构 $\Phi: E\to E$，当然 $\Phi\in\mathrm{Gal}(E/\mathbb{Q})$. 有两种可能：$\Phi(\sqrt{3})=\pm\sqrt{3}$. 事实上，现在易知 $\mathrm{Gal}(E/\mathbb{Q})$ 的元素对应于四群，它由恒等置换和下列三个置换（用轮换记号表示）组成：

$$(\sqrt{2},-\sqrt{2})(\sqrt{3},\sqrt{3}),(\sqrt{2},-\sqrt{2})(\sqrt{3},-\sqrt{3}),(\sqrt{2},\sqrt{2})(\sqrt{3},-\sqrt{3}).$$ ■

下面是伽罗瓦群的两个较一般的计算.

命题 4.11 如果 m 是正整数，k 是域，且如果 E 是 x^m-1 在 k 上的分裂域，则 $\mathrm{Gal}(E/k)$ 是阿贝尔群. 事实上，$\mathrm{Gal}(E/k)$ 同构于乘法群 $U(\mathbb{I}_m)$ 的一个子群，$U(\mathbb{I}_m)$ 是满足$(i,m)=1$ 的一切 $[i]$ 的乘法群.

证明 先假定 k 的特征不整除 m. 由例 4.6，E 包含一个 m 次单位原根 ω，从而 $E=k(\omega)$. E 中 x^m-1 的一切根的群是循环群，比如有生成元 ω，从而如果 $\sigma\in\mathrm{Gal}(E/k)$，则它的限制是循环群$\langle\omega\rangle$的自同构. 因此 $\sigma(\omega)=\omega^i$ 必也是$\langle\omega\rangle$ 的生成元，由定理 2.33（ⅰ），$(i,m)=1$. 易知 i 在 mod m 下是

唯一确定的，从而函数 $\varphi: \mathrm{Gal}(k(\omega)/k) \to U(\mathbb{I}_m)$（定义为如果 $\sigma(\omega)=\omega^i$，则 $\varphi(\sigma)=[i]$）是合理定义的. 现在 φ 是同态，这是因为如果 $\tau(\omega)=\omega^j$，则

$$\tau\sigma(\omega)=\tau(\omega^i)=(\omega^i)^j=\omega^{ij}.$$

204 最后，引理 4.2 表明 φ 是单射.

现在假设 k 有特征 p 且 $m=p^e n$，其中 $p \nmid n$. 由例 4.6，存在 n 次单位原根 ω，我们断言 $E=k(\omega)$ 是 x^m-1 的一个分裂域. 如果 $\zeta^m=1$，则 $1=\zeta^{p^e n}=(\zeta^n)^{p^e}$. 但因 k 有特征 p，因此 p^e 次单位根只有 1，所以 $\zeta^n=1$，即 $\zeta \in k(\omega)$. 于是简化成第一段的情形. [事实上，此时有更强的结果：$\mathrm{Gal}(E/k)$ 同构于乘法群 $U(\mathbb{I}_n)$ 的一个子群.] ■

注 *从命题我们不能得到如下的结论，即给定任一有限阿贝尔群 G，存在某个整数 m 使得 G 同构于 $U(\mathbb{I}_m)$ 的一个子群.*

定理 4.12 *如果 p 是素数，则*

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{I}_n,$$

*且一个生成元是***弗罗贝尼乌斯** $F: u \mapsto u^p$.

证明 设 $q=p^n$，$G=\mathrm{Gal}(\mathbb{F}_q /\!/ \mathbb{F}_p)$. 因为$\mathbb{F}_q$ 有特征 p，所以有 $(a+b)^p=a^p+b^p$，从而弗罗贝尼乌斯 F 是域的同态. 和任一域的同态一样，F 是单射. 因$\mathbb{F}_q$ 有限，根据习题 1.58，F 必是自同构；即 $F \in G$.

如果 $\pi \in \mathbb{F}_q$ 是一个本原元素，则由系 3.128，$d(x)=\mathrm{irr}(\pi, \mathbb{F}_p)$ 的次数为 n，从而根据定理 4.7(ii)，$|G|=n$. 只需证明 F 的阶 j 不小于 n. 如果对 $j<n$ 有 $F^j=1_{\mathbb{F}_q}$，则对于一切 $q=p^n$ 个元素 $u \in \mathbb{F}_q$ 有 $u^{p^j}=u$，这就给出多项式 $x^{p^j}-x$ 太多的根. ■

下面是引理 3.130 的一个优美推论，它说明在伽罗瓦理论和多边形的对称性之间的相似中，不可约多项式对应于正多边形.

命题 4.13 *设 k 是域，并设 $p(x) \in k[x]$ 无重根. 如果 E/k 是 $p(x)$ 的分裂域，则 $p(x)$ 是不可约的当且仅当 $\mathrm{Gal}(E/k)$ 传递地作用于 $p(x)$ 的根上.*

证明 假定 $p(x)$ 是不可约的，设 $\alpha, \beta \in E$ 是 $p(x)$ 的根. 根据定理 3.120（i），存在同构 $\varphi: k(\alpha) \to k(\beta)$ 使得 $\varphi(\alpha)=\beta$，且固定 k. 引理 3.130 证明，φ 可以扩张为 E 的固定 k 的自同构 Φ，即 $\Phi \in \mathrm{Gal}(E/k)$. 现在 $\Phi(\alpha)=\varphi(\alpha)=\beta$，从而 $\mathrm{Gal}(E/k)$ 传递地作用在根上.

反之，假定 $\mathrm{Gal}(E/k)$ 传递地作用在 $p(x)$ 的根上. 如果 $p(x)=q_1(x)\cdots q_t(x)$ 是分解为 $k[x]$ 中的不可约因式的因式分解，其中 $t \geq 2$，则选取 $q_1(x)$ 的一个根 $\alpha \in E$ 和 $q_2(x)$ 的一个根 $\beta \in E$. 由假设，存在 $\sigma \in \mathrm{Gal}(E/k)$ 使得 $\sigma(\alpha)=\beta$. 现在由命题 4.1，σ 置换 $q_1(x)$ 的根. 然而，因为 $p(x)$ 没有
205 重根，所以 β 不是 $q_1(x)$ 的根，这是一个矛盾. 所以 $t=1$，即 $p(x)$ 是不可约的. ■

现在可以给出系 4.9 的另一个证明. 定理 2.98 说，如果 X 是一个 G-集，则 $|G|=|\mathcal{O}(x)||G_x|$，其中$\mathcal{O}(x)$ 是 $x \in X$ 的轨道. 特别地，如果 X 是传递的G-集，则 $|X|$ 是 $|G|$ 的因数. 设 $f(x) \in k[x]$ 是可分不可约 n 次多项式，E/k 是它的分裂域. 如果 X 是 $f(x)$ 根的集合，则由命题 4.13，X 是传递的 $\mathrm{Gal}(E/k)$-集，从而，$n=\deg(f)=|X|$ 是 $|\mathrm{Gal}(E/k)|$ 的因数.

现在构成了对称群的一个类似物[⊖].

⊖ 实际上，更好的相似要涉及欧几里得空间$\mathbb{R}^n$ 中的多面体以代替只是平面中的多边形.

多边形 Ω……………………… 多项式 $f(x)\in k[x]$
正多边形 ……………………… 不可约多项式
Ω 的顶点 ……………………… $f(x)$ 的根
平面 ……………………… $f(x)$ 的分裂域 E
运动 ……………………… 固定 k 的自同构
对称群 $\Sigma(\Omega)$……………………… 伽罗瓦群 $\mathrm{Gal}(E/k)$

下面是基本策略．首先，我们把经典公式（给出高达 4 次的多项式的根）翻译为 k 上的分裂域 E 的子域的语言．其次，把已翻译的域的语言再翻译为群的语言：如果存在 $f(x)$的求根公式，则 $\mathrm{Gal}(E/k)$ 必是一个可解群（我们将立即定义）．最后，5 次和 5 次以上的多项式的伽罗瓦群可能不是可解的．结论是存在 5 次多项式没有与经典公式类似的求根公式．

4.1.1 求根公式与运用根式可解性

下面立即就把多项式求根公式的存在性翻译为分裂域的子域的语言．

定义 m **型纯扩张**是指扩张 $k(u)/k$，其中对某个 $m\geqslant 1$ 有 $u^m\in k$．称扩张 K/k 为**根式扩张**．如果存在域塔

$$k=K_0\subseteq K_1\subseteq\cdots\subseteq K_t=K,$$

其中每个 K_{i+1}/K_i 都是纯扩张．

如果 $u^m=a\in k$，则 $k(u)$ 是添加 a 的一个 m 次根到 k 得到的．如果 $k\subseteq\mathbb{C}$，则 a 有 m 个不同的根，即 $u,\omega u,\omega^2u,\cdots,\omega^{m-1}u$，其中 $\omega=\mathrm{e}^{2\pi i/m}$ 是 m 次单位原根．更一般地，如果 k 包含 m 次单位根，则 m 型纯扩张 $k(u)$，即 $u^m=a\in k$，是 x^m-a 的分裂域．并非$\mathbb{C}$的每个子域都包含一切单位根，例如$\mathbb{Q}$中的单位根只有 1 和 −1．因为要寻找的公式涉及开方，所以假定 k 包含适当的单位根总归是有利的．

206

当说到多项式 $f(x)$ 存在类似二次公式那样的求根公式时，我们的意思是用 $f(x)$ 的系数组成的表达式给出 $f(x)$ 的根．这个表达式可以使用域的运算、常数和开方，但不涉及用到余弦、定积分或极限一类的其他运算．当我们提出 $f(x)$ 运用根式可解后，上面非正式描述的那种求根公式可以精确化，现在定义 $f(x)$ 运用根式可解．

定义 设 $f(x)\in k[x]$ 有分裂域 E．如果存在根式扩张

$$k=K_0\subseteq K_1\subseteq\cdots\subseteq K_t$$

使得 $E\subseteq K_t$，我们说 $f(x)$ **运用根式可解**．

对每一个域 k 和每一个 $m\geqslant 1$，我们证明多项式 $f(x)=x^m-1\in k[x]$ 运用根式可解．回忆由 $f(x)$ 的分裂域 E/k 中的所有 m 次单位根组成的集合 Γ_m 是循环群，比如说具有生成元 ζ．注意 $|\Gamma_m|=m$，除非 k 有特征 $p>0$ 且 $p\mid m$，此时 $|\Gamma_m|=m'$，其中 $m=p^em'$ 且 $p\nmid m'$．现在 $E=k(\zeta)$，因此 E 是 k 的纯扩张，从而 E/k 是根式扩张．于是，$f(x)=x^m-1$ 运用根式可解．

下面通过考虑小次数多项式的经典公式来解释这个定义．

二次多项式

如果 $f(x)=x^2+bx+c$，则二次公式给出它的根为

$$\frac{1}{2}\left(-b\pm\sqrt{b^2-4c}\right).$$

令 $k=\mathbb{Q}(b,c)$. 定义 $K_1=k(u)$，其中 $u=\sqrt{b^2-4c}$. 则 K_1 是 k 的根式扩张，因为 $u^2\in k$. 此外，二次公式蕴涵 K_1 是 $f(x)$ 的分裂域，所以 $f(x)$ 运用根式可解.

三次多项式

设 $f(X)=X^3+bX^2+cX+d$,令 $k=\mathbb{Q}(b,c,d)$. 作变量替换 $X=x-\frac{1}{3}b$ 产生一个新多项式 $\tilde{f}(x)=x^3+qx+r\in k[x]$，它和 $f(X)$ 有相同的分裂域 E [因为如果 u 是 $\tilde{f}(x)$ 的根，则 $u-\frac{1}{3}b$ 是 $f(x)$ 的根]，从而 $\tilde{f}(x)$ 运用根式可解当且仅当 $f(x)$ 运用根式可解. 1515 年 Scipio del Ferro 发现了三次公式的一个特殊情形，1535 年 Niccolò Fontana (Tartaglia) 和 1545 年 Giralamo Cardano 完成了剩下的情形. 三次公式给出 $\tilde{f}(x)$ 的根为

207

$$g+h,\omega g+\omega^2 h,\omega^2 g+\omega h,$$

其中 $g^3=\frac{1}{2}(-r+\sqrt{R}),h=-q/3g,R=r^2+\frac{4}{27}q^3,\omega=-\frac{1}{2}+\mathrm{i}\frac{\sqrt{3}}{2}$ 是一个三次单位原根.

三次公式是如下导出的. 如果 u 是 $\tilde{f}(x)=x^3+qx+r$ 的一个根，记

$$u=g+h.$$

并代入得：

$$0=\tilde{f}(u)=\tilde{f}(g+h)=g^3+h^3+(3gh+q)u+r.$$

现在二次公式可以改述为：给定任意一对数 u,v, 存在（可能是复数）数 g,h 使得 $u=g+h,v=gh$. 所以可以进一步假定 $3gh+q=0$，即

$$g^3+h^3=-r,gh=-\frac{1}{3}q.$$

三次方后一个式子，得一对方程：

$$g^3+h^3=-r$$

$$g^3h^3=-\frac{1}{27}q^3,$$

由此得到 g^3 的二次方程：

$$g^6+rg^3-\frac{1}{27}q^3=0.$$

二次公式给出

$$g^3=\frac{1}{2}\left(-r+\sqrt{r^2+\frac{4}{27}q^3}\right)=\frac{1}{2}(-r+\sqrt{R})$$

[注意 h^3 也是这个二次多项式的根，从而 $h^3=\frac{1}{2}(-r-\sqrt{R})$]. g^3 有三个三次根：$g,\omega g$ 和 $\omega^2 g$. 因为有约束 $gh=-\frac{1}{3}q$，所以它们每个都有一个"配偶"，就是 $h=-q/(3g)$，$-q/(3\omega g)=\omega^2 h$ 和 $-q/(3\omega^2 g)=\omega h$.

现在来看 $\tilde{f}(x)$ 是运用根式可解的. 定义 $K_1=k(\sqrt{R})$，其中 $R=r^2+\frac{4}{27}q^3$，$K_2=K_1(\alpha)$，其中 $\alpha^3=\frac{1}{2}(-r+\sqrt{R})$. 三次公式表明 K_2 包含 $\tilde{f}(x)$ 的根 $\alpha+\beta$，其中 $\beta=-q/3\alpha$. 最后定义 $K_3=$

$K_2(\omega)$，其中 $\omega^3=1$. $\tilde{f}(x)$ 其他的根是 $\omega\alpha+\omega^2\beta$ 和 $\omega^2\alpha+\omega\beta$，两者都在 K_3 中，从而 $E\subseteq K_3$.

一个分裂域 E 未必等于 K_3，这是因为如果 $f(x)$ 的一切根都是实数，则 $E\subseteq\mathbb{R}$，而 $K_3\nsubseteq\mathbb{R}$. 三次公式一个有趣的方面是所谓的不可约案例，即对于$\mathbb{Q}[x]$ 中一个有全部实根的三次不可约多项式，求根公式需要出现复数.（见罗特曼所著的《Galois Theory》，第二版，99 页）.

不可约案例 如果 $f(x)=x^3+qx+r\in\mathbb{Q}[x]$ 是一个不可约多项式，它有三个实根，则任一包含 $f(x)$ 的分裂域的根式扩张 $K_t/\mathbb{Q}$ 不是实数域，即 $K_t\nsubseteq\mathbb{R}$.

208

例 4.14 如果 $f(x)=x^3-15x-126$，则 $q=-15$，$r=-126$，$R=15\ 376$，$\sqrt{R}=124$. 因此 $g^3=125$，从而 $g=5$. 由此 $h=-q/(3g)=1$. 所以 $f(x)$ 的根是

$$6,5\omega+\omega^2=-3+2\mathrm{i}\sqrt{3},5\omega^2+\omega=-3-2\mathrm{i}\sqrt{3}.$$

另一种方法，如果已经求出一个根为 6，其他两个根可以作为二次多项式 $f(x)/(x-6)=x^2+6x+21$ 的根求出来. ■

例 4.15 三次公式用处不大，因为它给出的根常常处于无法辨别的形式. 例如，设

$$f(x)=(x-1)(x-2)(x+3)=x^3-7x+6.$$

三次公式给出

$$g+h=\sqrt[3]{\frac{1}{2}\left(-6+\sqrt{\frac{-400}{27}}\right)}+\sqrt[3]{\frac{1}{2}\left(-6-\sqrt{\frac{-400}{27}}\right)}.$$

根本看不出 $g+h$ 是实数，更不用说是一个整数. 三次公式还有另一种形式，它属于 F. Viète，他给出的根用三角函数代替根式（见我的书《A First Course in Abstract Algebra》360～362 页）. ■

四次多项式

设 $f(X)=X^4+bX^3+cX^2+dX+e$，令 $k=\mathbb{Q}(b,c,d,e)$. 作变量替换 $X=x-\frac{1}{4}b$ 产生新多项式 $\tilde{f}(x)=x^4+qx^2+rx+s\in k[x]$. 此外，如果 u 是 $\tilde{f}(x)$ 的根，则 $u-\frac{1}{4}b$ 是 $f(x)$ 的根，所以 $f(x)$ 的分裂域等于 $\tilde{f}(x)$ 的分裂域. 四次公式于 1545 年由 Luigi Ferrari 发现，但下面的形式是 1637 年笛卡儿（R. Descartes）提出的. 在 $\mathbb{C}[x]$ 中分解 $\tilde{f}(x)$：

$$\tilde{f}(x)=x^4+qx^2+rx+s=(x^2+jx+\ell)(x^2-jx+m),$$

并确定 j,ℓ,m. 展开后由同次项系数相等得方程

$$\begin{aligned}\ell+m-j^2&=q;\\ j(m-\ell)&=r;\\ \ell m&=s.\end{aligned}$$

前两个方程给出

$$\begin{aligned}2m&=j^2+q+r/j;\\ 2\ell&=j^2+q-r/j.\end{aligned}$$

209

用这些值替换第三个方程中的 m，ℓ 产生**预解三次多项式**：

$$(j^2)^3+2q(j^2)^2+(q^2-4s)j^2-r^2.$$

三次公式给出 j^2，由此可确定 m 和ℓ，从而得到四次多项式的根.

和三次多项式的情形一样，定义纯扩张

$$k=K_0\subseteq K_1\subseteq K_2\subseteq K_3,$$

从而 $j^2 \in K_3$. 定义 $K_4 = K_3(j)$(从而 $m, \ell \in K_4$). 最后定义 $K_5 = K_4(\sqrt{j^2 - 4\ell})$ 和 $K_6 = K_5(\sqrt{j^2-4m})$ [给出 $\tilde{f}(x)$ 的二次因式 $x^2 + jx + \ell$ 和 $x^2 - jx + m$ 的根]. 四次公式给出 $E \subseteq K_6$.

刚才已经看到二次多项式、三次多项式和四次多项式是运用根式可解的. 反之, 如果 $f(x)$ 是运用根式可解的多项式, 则存在所要求的那种用它的系数表示它的根的公式. 假设

$$k = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_t$$

是根式扩张使得分裂域 $E \subseteq K_t$, 令 z 是 $f(x)$ 的一个根. 现在 $K_t = K_{t-1}(u)$, 其中 u 是某个元素 $\alpha \in K_{t-1}$ 的 m 次根; 因此 z 可用 u 和 K_{t-1} 表示; 即 z 可用 $\sqrt[m]{\alpha}$ 和 K_{t-1} 表示. 但 $K_{t-1} = K_{t-2}(v)$, 其中 v 的某个幂在 K_{t-2} 中. 因此 z 可用 u, v 和 K_{t-2} 表示. 最终, z 可由类似于那些经典公式的一个公式表示.

4.1.2 转化为群论

这个策略的第二步涉及研究 $f(x)$ 运用根式可解对它的伽罗瓦群的影响.

假设 $k(u)/k$ 是 6 型纯扩张, 即 $u^6 \in k$. 现在 $k(u^3)/k$ 是 2 型纯扩张, 因为 $(u^3)^2 = u^6 \in k$, 而 $k(u)/k(u^3)$ 显然是 3 型纯扩张. 于是 $k(u)/k$ 可以换成 2 型和 3 型纯扩张的塔 $k \subseteq k(u^3) \subseteq k(u)$. 更一般地, 可以假定给定一个纯扩张的塔, 每个域是它前一个上的素数型纯扩张: 如果 $k \subseteq k(u)$ 是 m 型的, 则分解 m 为 $m = p_1 \cdots p_q$, 其中所有 p (不必不同) 都是素数, 把 $k \subseteq k(u)$ 替换为

$$k \subseteq k(u^{m/p_1}) \subseteq k(u^{m/p_1 p_2}) \subseteq \cdots \subseteq k(u).$$

下面是关键结果, 它可以把运用根式的可解性转化为伽罗瓦群的语言.

定理 4.16 *设 $k \subseteq B \subseteq E$ 是一个域塔, $f(x), g(x) \in k[x]$, B 是 $f(x)$ 在 k 上的一个分裂域, E 是 $g(x)$ 在 k 上的一个分裂域, 则 $\mathrm{Gal}(E/B)$ 是 $\mathrm{Gal}(E/k)$ 的正规子群, 且*

210

$$\mathrm{Gal}(E/k)/\mathrm{Gal}(E/B) \cong \mathrm{Gal}(B/k).$$

证明 设 $B = k(z_1, \cdots, z_t)$, 其中 $z_1, \cdots, z_t$ 是 $f(x)$ 在 E 中的根. 如果 $\sigma \in \mathrm{Gal}(E/k)$, 则根据命题 4.1(ⅰ), σ 置换 $z_1, \cdots, z_t$ (因为 σ 固定 k), 从而 $\sigma(B) = B$. 定义 $\rho: \mathrm{Gal}(E/k) \to \mathrm{Gal}(B/k)$ 为 $\sigma \mapsto \sigma | B$. 如同定理 4.3 的证明, 易知 ρ 是同态且 $\ker\rho = \mathrm{Gal}(E/B)$. 由此, $\mathrm{Gal}(E/B)$ 是 $\mathrm{Gal}(E/k)$ 的正规子群. 但 ρ 是满射: 如果 $\tau \in \mathrm{Gal}(B/k)$, 则根据引理 3.130, 存在 $\sigma \in \mathrm{Gal}(E/k)$ 是 τ 的扩张 [即 $\rho(\sigma) = \sigma | B = \tau$]. 由第一同构定理, 定理得证. ■

当应用定理 4.16 的时候, 需要用到下面一个技术性的结果.

引理 4.17 (ⅰ) *如果 $B = k(\alpha_1, \cdots, \alpha_n)$ 是域 k 的一个有限扩张, 则存在有限扩张 E/B 使得 E/B 成为某个多项式 $f(x) \in k[x]$ 的分裂域 (次数最低的这种扩张叫做 B/k 的**正规**[⊖]**闭包**). 此外, 如果每个 α_i 在 k 上可分, 则可选取 $f(x)$ 为可分多项式.*

(ⅱ) *如果 B 是 k 的根式扩张, 则 (ⅰ) 中的扩张 E/k 是 k 的根式扩张.*

证明 (ⅰ) 根据定理 3.120 (ⅰ), 在 $k[x]$ 中存在不可约多项式 $p_i(x) = \mathrm{irr}(\alpha_i, k)$ 使得对每个 i 有 $p_i(\alpha_i) = 0$, 且有 $f(x) = p_1(x) \cdots p_n(x)$ 的分裂域 E 包含 B. 如果每个 α_i 在 k 上可分, 则每个 $p_i(x)$ 是可分多项式, 因此 $f(x)$ 是可分多项式.

(ⅱ) 对任一多项式 $p_i(x)$ 的每一对根 α 和 α', 存在同构 $\gamma: k(\alpha) \to k(\alpha')$, 它固定 k, 且把 $\alpha \mapsto \alpha'$, 这是因为 $k(\alpha)$ 和 $k(\alpha')$ 都同构于 $k[x]/(p_i(x))$. 根据引理 3.130, 每个这样的 γ 可以扩张为一个自同构 $\sigma \in G = \mathrm{Gal}(E/k)$. 从而 $E = k(\sigma(u_1), \cdots, \sigma(u_t) : \sigma \in G)$.

⊖ 如果扩张 E/k 是 $k[x]$ 中某个多项式集合的分裂域, 则常称 E/k 为**正规扩张**.

如果 B/k 是根式扩张，则

$$k \subseteq k(u_1) \subseteq k(u_1, u_2) \subseteq \cdots \subseteq k(u_1, \cdots, u_t) = B,$$

其中每个 $k(u_1, \cdots, u_{i+1})$ 是 $k(u_1, \cdots, u_i)$ 的纯扩张．当然，对每个 $\sigma \in G, \sigma(B) = k(\sigma(u_1), \cdots, \sigma(u_t))$ 是 k 的根式扩张．现在证明 E 是 k 的根式扩张．定义

$$B_1 = k(\sigma(u_1) : \sigma \in G).$$

现在如果 $G = \{1, \sigma, \tau, \cdots\}$，则域塔

$$k \subseteq k(u_1) \subseteq k(u_1, \sigma(u_1)) \subseteq k(u_1, \sigma(u_1), \tau(u_1)) \subseteq \cdots \subseteq B_1$$

表明 B_1 是 k 的一个根式扩张．例如，如果 u_1^m 在 k 中，则 $\tau(u_1)^m = \tau(u_1^m)$ 在 $\tau(k) = k$ 中，因此 $\tau(u_1)^m$ 在 $k \subseteq (u_1, \sigma(u_1))$ 中．由归纳假设，假定已经构造了一个根式扩张 B_i/k，它包含一切满足 $j \leqslant i$ 的 $\{\sigma(u_j) : \sigma \in G\}$．定义 [211]

$$B_{i+1} = B_i(\sigma(u_{i+1}) : \sigma \in G).$$

易知 B_{i+1}/B_i 是根式扩张：如果 $u_{i+1}^m \in k(u_1, \cdots, u_i)$，则 $\tau(u_{i+1})^m \in k(\tau(u_1), \cdots \tau(u_i)) \subseteq B_i$，从而 B_{i+1} 是 k 的根式扩张．最后，因 $E = B_t$，从而证明 E 是 k 的根式扩张．■

现在给出我们所一直寻找的翻译的核心．

引理 4.18 设

$$K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_t$$

是域 K_0 的一个根式扩张．假定对每个 $i \geqslant 1, K_i$ 是 K_{i-1} 上的素数 p_i 型纯扩张，其中 $p_i \neq \mathrm{char}(K_0)$，且 K_0 包含所有 p_i 次单位根．如果 K_t 是 K_0 上的分裂域，则存在子群序列

$$\mathrm{Gal}(K_t/K_0) = G_0 \geqslant G_1 \geqslant G_2 \geqslant \cdots \geqslant G_t = \{1\},$$

其中每个 G_{i+1} 是 G_i 的正规子群，且 G_i/G_{i+1} 是素数 p_{i+1} 阶循环群．

证明 对每个 i，定义 $G_i = \mathrm{Gal}(K_t/K_i)$．显然

$$\mathrm{Gal}(K_t/K_0) = G_0 \geqslant G_1 \geqslant G_2 \geqslant \cdots \geqslant G_t = \{1\}$$

是一个子群序列．因 $K_1 = K_0(u)$，其中 $u^{p_1} \in K_0, \mathrm{char}(K_0) \neq p_1$ 和 K_0 包含一切 p_1 次单位根的假设蕴涵 K_0 包含一个 p_1 次单位原根 ω．因为 $u, \omega u, \cdots, \omega^{p_1-1}u$ 是多项式 $x^{p_1} - u^{p_1}$ 的根，所以 K_1 是可分多项式 $x^{p_1} - u^{p_1}$ 的分裂域．现在应用定理 4.16 可知，$G_1 = \mathrm{Gal}(K_t/K_1)$ 是 $G_0 = \mathrm{Gal}(K_t/K_0)$ 的正规子群，且 $G_0/G_1 \cong \mathrm{Gal}(K_1/K_0)$．根据定理 4.7（ⅱ），$G_0/G_1 \cong \mathbb{I}_{p_1}$．该论证可对每个 i 重复进行．■

引理 4.18 导出下面的定义．

定义 *群 G 的***正规列**[⊖]*是指子群序列*

$$G = G_0 \geqslant G_1 \geqslant G_2 \geqslant \cdots \geqslant G_t = \{1\},$$

*其中每个 G_{i+1} 是 G_i 的正规子群，该序列的***因子群***是指商群*

$$G_0/G_1, G_1/G_2, \cdots, G_{n-1}/G_n.$$

*称有限群 G 是***可解群***，如果它有一个正规列，且该正规列的每个因子群的阶都是素数（无限可解群*

⊖ 该术语并不十分标准．我们知道正规性是不传递的，即如果 $H \leqslant K$ 是群 G 的子群，则 $H \lhd K$，而 $K \lhd G$ 未必有 $H \lhd G$．称子群 $H \leqslant G$ 为**次正规子群**，如果存在链

$$G = G_0 \geqslant G_1 \geqslant G_2 \geqslant \cdots \geqslant G_t = H,$$

其中对一切 $i \geqslant 1, G_i \lhd G_{i-1}$．本课文中定义的正规列有些作者称之为**次正规列**，他们把正规列的名称留给这样的序列，即其中每个 G_i 都是大群 G 的正规子群．

212 的定义见 286 页).

用该定义的说法，引理 4.18 就是：如果 K_t 是 K_0 的根式扩张且 K_0 包含适当的单位根，则 $\mathrm{Gal}(K_t/K_0)$ 是可解群.

例 4.19 (i) 根据习题2.86(ii)，每个有限阿贝尔群 G 有指数为素数的子群（必定是正规的），从而可对 $|G|$ 用归纳法推出每个有限阿贝尔群都是可解群.

(ii) 证明 S_4 是一个可解群. 考虑子群链

$$S_4 \geqslant A_4 \geqslant \mathbf{V} \geqslant W \geqslant \{1\},$$

其中 $\mathbf{V}$ 是四-群，W 是 $\mathbf{V}$ 的任一个 2 阶子群. 注意，因为 $\mathbf{V}$ 是阿贝尔群，所以 W 是 $\mathbf{V}$ 的正规子群. 现在 $|S_4/A_4| = |S_4|/|A_4| = 24/12 = 2$，$|A_4/\mathbf{V}| = |A_4|/|\mathbf{V}| = 12/4 = 3$，$|\mathbf{V}/W| = |\mathbf{V}|/|W| = 4/2 = 2$ 以及 $|W/\{1\}| = |W| = 2$. 因每个因子群的阶都是素数，S_4 是可解群.

(iii) 一个非阿贝尔单群 G 是不可解的，例如 $G = A_5$，因为它唯一的真正规子群是 $\{1\}$，且 $G/\{1\} \cong G$ 不是素数阶循环群. ■

下一引理中关于单位根的笨拙假设将很快被移除.

引理 4.20 *设 k 是域，并设 $f(x) \in k[x]$ 运用根式可解，从而存在根式扩张 $k = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_t$，其中 K_t 包含 $f(x)$ 的一个分裂域 E. 如果每个 K_i/K_{i-1} 是一个素数 p_i 型纯扩张，其中 $p_i \neq \mathrm{char}(k)$，且如果 k 包含所有 p_i 次单位根，则伽罗瓦群 $\mathrm{Gal}(E/k)$ 是一个可解群的商群.*

证明 存在素数型纯扩张的塔

$$k = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_t,$$

其中 $E \subseteq K_t$. 根据引理 4.17，可假设 K_t 也是 $k[x]$ 中的某个多项式的分裂域. 关于 k 的假设使得能够应用引理 4.18 得知 $\mathrm{Gal}(K_t/k)$ 是可解群. 因为 E 和 K_t 都是 k 上的分裂域，定理 4.16 给出所要证明的 $\mathrm{Gal}(K_t/k)/\mathrm{Gal}(K_t/E) \cong \mathrm{Gal}(E/k)$. ■

命题 4.21 *可解群 G 的每个商群 G/N 也是可解群.*

证明 设 $G = G_0 \geqslant G_1 \geqslant G_2 \geqslant \cdots \geqslant G_t = \{1\}$ 是可解群定义中的子群序列. 因为 $N \lhd G$，对所有 i，NG_i 是 G 的子群，从而有子群序列

$$G = G_0N \geqslant G_1N \geqslant \cdots \geqslant G_tN = N \geqslant \{1\}.$$

这是一个正规列：利用明显的记号，

213
$$(g_in)G_{i+1}N(g_in)^{-1} \leqslant g_iG_{i+1}Ng_i^{-1} = g_iG_{i+1}g_i^{-1}N \leqslant G_{i+1}N;$$

第一个不等式成立是因为 $n(G_{i+1}N)n^{-1} \leqslant NG_{i+1}N \leqslant (G_{i+1}N)(G_{i+1}N) = G_{i+1}N$（因 $G_{i+1}N$ 是子群）；等式成立是因为 $Ng_i^{-1} = g_i^{-1}N$（因 $N \lhd G$，从而它的右陪集等于它的左陪集）；最后一个不等式成立是因为 $G_{i+1} \lhd G_i$.

第二同构定理给出

$$\frac{G_i}{G_i \cap (G_{i+1}N)} \cong \frac{G_i(G_{i+1}N)}{G_{i+1}N} = \frac{G_iN}{G_{i+1}N},$$

最后一个等式成立是因为 $G_iG_{i+1} = G_i$. 因 $G_{i+1} \lhd G_i \cap G_{i+1}N$，第三同构定理给出满射 $G_i/G_{i+1} \to G_i/[G_i \cap G_{i+1}N]$，从而复合是满射 $G_i/G_{i+1} \to G_iN/G_{i+1}N$. 因 G_i/G_{i+1} 是素数阶循环群，它的象不是素数阶循环群就是平凡群. 所以 G/N 是可解群. ■

命题 4.22 *可解群 G 的每个子群 H 是可解群.*

证明 因 G 是可解群，存在子群序列

$$G = G_0 \geqslant G_1 \geqslant G_2 \geqslant \cdots \geqslant G_t = \{1\},$$

其中对所有 i，G_i 是 G_{i-1} 中的正规子群，且 G_{i-1}/G_i 是循环群. 考虑子群序列

$$H = H \cap G_0 \geqslant H \cap G_1 \geqslant H \cap G_2 \geqslant \cdots \geqslant H \cap G_t = \{1\}.$$

这是一个正规列：如果 $h_{i+1} \in H \cap G_{i+1}$ 且 $g_i \in H \cap G_i$，则因为 $g_i, h_{i+1} \in H$，从而 $g_i h_{i+1} g_i^{-1} \in H$. 因为 G_{i+1} 是 G_i 中的正规子群，也有 $g_i h_{i+1} g_i^{-1} \in G_{i+1}$. 所以 $g_i h_{i+1} g_i^{-1} \in H \cap G_{i+1}$，从而 $H \cap G_{i+1} \lhd H \cap G_i$. 最后，第二同构定理给出

$$(H \cap G_i)/(H \cap G_{i+1}) = (H \cap G_i)/[(H \cap G_i) \cap G_{i+1}]$$
$$\cong G_{i+1}(H \cap G_i)/G_{i+1}.$$

而最后一个（商）群是 G_i/G_{i+1} 的子群. 因一个素数阶循环群 C 的子群只有 C 和 $\{1\}$，从而非平凡的因子群 $(H \cap G_i)/(H \cap G_{i+1})$ 是素数阶循环群. 所以 H 是可解群. ■

例 4.23 在例4.19(ⅱ)中，我们证明了 S_4 是可解群. 然而，如果 $n \geqslant 5$，对称群 S_n 不是可解群. 相反，如果 S_n 是可解群，则它的每个子群也是可解群. 但 $A_5 \leqslant S_5 \leqslant S_n$，且 A_5 不是可解群，因为它是一个非阿贝尔单群. ■

命题 4.24 *如果 $H \lhd G$ 且 H 和 G/H 两者都是可解群，则 G 是可解群.*

证明 因 G/H 是可解的，存在正规列

$$G/H \geqslant K_1^* \geqslant K_2^* \geqslant \cdots K_m^* = \{1\}$$

[214]

具有素数阶因子群. 根据群的对应定理，存在 G 的子群 K_i，

$$G \geqslant K_1 \geqslant K_2 \geqslant \cdots \geqslant K_m = H,$$

其中对一切 $i, K_i/H = K_i^*$ 且 $K_{i+1} \lhd K_i$. 根据第三同构定理，对一切 i，

$$K_i^* / K_{i+1}^* \cong K_i/K_{i+1},$$

从而对一切 $i, K_i/K_{i+1}$ 是素数阶循环群.

因 H 是可解群，存在正规列

$$H \geqslant H_1 \geqslant H_2 \geqslant \cdots H_q = \{1\}$$

具有素数阶因子群. 把两个序列连接起来，

$$G \geqslant K_1 \geqslant K_2 \geqslant \cdots \geqslant K_m \geqslant H_1 \geqslant H_2 \geqslant \cdots H_q = \{1\},$$

得到 G 的有素数阶因子群的正规列. ■

系 4.25 *如果 H 和 K 是可解群，则 $H \times K$ 也是可解群.*

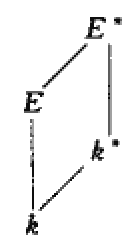
证明 因 $(H \times K)/H \cong K$，从命题 4.24 立刻得到结果. ■

回到域，我们现在可以给出判别一个多项式运用根式可解的主要准则.

定理 4.26（伽罗瓦） *设 $f(x) \in k[x]$，其中 k 是域，并设 E 是 $f(x)$ 在 k 上的分裂域. 如果 $f(x)$ 是运用根式可解的，则它的伽罗瓦群 $\mathrm{Gal}(E/k)$ 是可解群.*

注 *当 k 有特征 $p>0$ 时，逆定理不成立（见命题 4.56），但当 k 有特征 0 时，逆定理成立（见定理 4.53）.*

证明 在引理 4.20 的证明中，假定基础域包含某些 p_i 次单位根（素数 p_i 是纯扩张的类型）. 定义 m 为所有这些 p_i 的积，定义 E^* 是 x^m-1 在 E 上的分裂域，并定义 $k^* = k(\Omega)$，其中 Ω 是 E^* 中所有 m 次单位根的集合. 现在 E^* 是 $f(x)$ 在 k^* 上的分裂域，从而根据命题 4.21，$\mathrm{Gal}(E^*/k^*)$ 是可解群.



215

考虑塔 $k \subseteq k^* \subseteq E^*$，根据定理 4.16，有 $\mathrm{Gal}(E^*/k^*) \lhd \mathrm{Gal}(E^*/k)$，且

$$\mathrm{Gal}(E^*/k)/\mathrm{Gal}(E^*/k^*) \cong \mathrm{Gal}(k^*/k).$$

现在 $\mathrm{Gal}(E^*/k^*)$ 是可解群，而 $\mathrm{Gal}(k^*/k)$ 是阿贝尔群，从而根据命题 4.11，它也是可解群；所以根据命题 4.24，$\mathrm{Gal}(E^*/k)$ 是可解群. 最后，因为塔 $k \subseteq E \subseteq E^*$ 满足 E 和 E^* 都是 $k[x]$ 中多项式的分裂域[E^* 是 $(x^m-1)f(x)$ 的分裂域] 的假设条件，我们可以再一次应用定理 4.16. 由此得到 $\mathrm{Gal}(E^*/k)/\mathrm{Gal}(E^*/E) \cong \mathrm{Gal}(E/k)$，因 $\mathrm{Gal}(E/k)$ 是可解群的商群，从而 $\mathrm{Gal}(E/k)$ 是可解群. ■

回忆如果 k 是域，$E = k(y_1,\cdots,y_n) = \mathrm{Frac}(k[y_1,\cdots,y_n])$ 是有理函数域，则 k 上 n 次一般多项式是

$$(x-y_1)(x-y_2)\cdots(x-y_n).$$

伽罗瓦定理足以证明一般五次多项式不存在二次公式的推广.

定理 4.27 (阿贝尔-鲁菲尼)　*如果 $n \geqslant 5$，则域 k 上的 n 次一般多项式*

$$f(x) = (x-y_1)(x-y_2)\cdots(x-y_n)$$

不是运用根式可解的.

证明　在例 3.125 中可以看到，如果 $E = k(y_1,\cdots,y_n)$ 是系数在域 k 中一切 n 个变量的有理函数的域，又如果 $F = k(a_0,\cdots,a_{n-1})$，其中 a_i 是 $f(x)$ 的系数，则 E 是 $f(x)$ 在 F 上的分裂域.

我们断言 $\mathrm{Gal}(E/F) \cong S_n$. 习题 3.47(ⅰ)说明如果 A 和 R 是整环且 $\varphi: A \to R$ 是同构，则 $a/b \mapsto \varphi(a)/\varphi(b)$ 是同构 $\mathrm{Frac}(A) \to \mathrm{Frac}(R)$. 特别地，如果 $\sigma \in S_n$，则存在由 $\tilde{\sigma}: f(y_1,\cdots,y_n) \mapsto f(y_{\sigma 1},\cdots,y_{\sigma n})$ 定义的 $k[y_1,\cdots,y_n]$ 的自同构 $\tilde{\sigma}$；即 $\tilde{\sigma}$ 恰好置换各变量，且 $\tilde{\sigma}$ 可以扩张为 $E = \mathrm{Frac}(k[y_1,\cdots,y_n])$ 的自同构 σ^*. 198 页等式 (1) 表明 σ^* 固定 F，从而 $\sigma^* \in \mathrm{Gal}(E/F)$. 由引理 4.2 易知 $\sigma \mapsto \sigma^*$ 是单射 $S_n \to \mathrm{Gal}(E/F)$，从而 $|S_n| \leqslant |\mathrm{Gal}(E/F)|$. 另一方面，定理 4.3 表明 $\mathrm{Gal}(E/F)$ 可以嵌入 S_n，从而给出反过来的不等式 $|\mathrm{Gal}(E/F)| \leqslant |S_n|$. 所以 $\mathrm{Gal}(E/F) \cong S_n$. 但根据例 4.23，当 $n \geqslant 5$ 时 S_n 不是可解群，从而定理 4.26 表明 $f(x)$ 不是运用根式可解的. ■

我们知道 $\mathbb{Q}[x]$ 中的某些五次多项式是运用根式可解的，例如 x^5-1 是运用根式可解的，这是因为根据命题 4.11，它的伽罗瓦群是阿贝尔群. 另一方面，可以给出 $\mathbb{Q}[x]$ 中的特定的五次多项式，它不是运用根式可解的. 例如 $f(x) = x^5-4x+2 \in \mathbb{Q}[x]$ 不是运用根式可解的，这是因为可以证明它的伽罗瓦群同构于 S_5（见习题 4.13).

216

习题

4.1　给定 $u, v \in \mathbb{C}$，证明存在 $g, h \in \mathbb{C}$ 使得 $u = g+h, v = gh$.

4.2　证明当 k 的特征等于 2 时，二次公式对 $ax^2+bx+c \in k[x]$ 不成立.

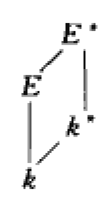
4.3　(ⅰ) 求 $f(x) = x^3-3x+1 \in \mathbb{Q}[x]$ 的根.

(ⅱ) 求 $f(x) = x^4-2x^2+8x-3 \in \mathbb{Q}[x]$ 的根.

4.4　设 $f(x) \in E[x]$ 并假设 $f(x)$ 是首一多项式，其中 E 是域，并设 $\sigma: E \to E$ 是自同构. 如果 $f(x)$ 分裂且 σ

固定 $f(x)$ 的每个根，证明 σ 固定 $f(x)$ 的每个系数.

4.5 (**配连无理性**) 设 E/k 是 $f(x) \in k[x]$ 的分裂域且伽罗瓦群 $G = \mathrm{Gal}(E/k)$. 证明：如果 k^*/k 是域扩张，且 E^* 是 $f(x)$ 在 k^* 上的分裂域



则限制 $\sigma \mapsto \sigma \mid E$ 是单同态

$$\mathrm{Gal}(E^*/k^*) \to \mathrm{Gal}(E/k).$$

提示：如果 $\sigma \in \mathrm{Gal}(E^*/k^*)$，则 σ 置换 $f(x)$ 的根，从而 $\sigma \mid E \in \mathrm{Gal}(E/k)$.

4.6 (i) 设 E/k 是域扩张，$f(x) \in k[x]$ 是可分多项式. 证明：当把 $f(x)$ 看作 $K[x]$ 中的多项式时，$f(x)$ 仍是可分多项式.

(ii) 设 k 是域，$f(x), g(x) \in k[x]$. 证明：如果 $f(x)$ 和 $g(x)$ 都是可分多项式，则它们的积也是可分多项式.

4.7 设 k 是域，$f(x) \in k[x]$ 是可分多项式. 如果 E/k 是 $f(x)$ 的分裂域，证明 $f(x)$ 在 E 中的每个根都是 k 上的可分元素.

4.8 设域扩张 K/k 是多项式 $f(x) \in k[x]$ 的分裂域. 如果 $p(x) \in k[x]$ 是无重根的首一不可约多项式，且在 $K[x]$ 中，

$$p(x) = g_1(x) \cdots g_r(x),$$

其中 $g_i(x)$ 是 $K[x]$ 中的首一不可约多项式，证明所有 $g_i(x)$ 的次数相同. 由此可知 $\deg(p) = r\deg(g_i)$.

提示：在 $p(x)f(x)$ 的某个分裂域 E/K 中，设 α 是 $g_i(x)$ 的一个根，β 是 $g_j(x)$ 的一个根，其中 $i \neq j$. 存在同构 $\varphi: k(\alpha) \to k(\beta)$ 满足 $\varphi(\alpha) = \beta$ 而固定 k，且 φ 可扩张为 $\Phi: E \to E$. 证明 $\Phi \mid K$ 导出 $K[x]$ 的一个自同构把 $g_i(x)$ 变到 $g_j(x)$.

4.9 (i) 举出一个群 G 的例子，它有不是正规子群的次正规子群.

(ii) 举出一个群 G 的例子，它有不是次正规子群的子群.

217

4.10 证明对于二次多项式 $f(x) = ax^2 + bx + c \in \mathbb{Q}[x]$，下列陈述等价.

(i) $f(x)$ 在 $\mathbb{Q}[x]$ 中不可约.

(ii) $\sqrt{b^2 - 4ac}$ 不是有理数.

(iii) $\mathrm{Gal}(\mathbb{Q}(\sqrt{b^2 - 4ac})/\mathbb{Q})$ 的阶为 2.

4.11 (i) 设 k 是域，$f(x) \in k[x]$ 是 p 次多项式，其中 p 是素数，并设 E/k 为 $f(x)$ 的分裂域. 证明：如果 $\mathrm{Gal}(E/k) \cong \mathrm{I}_p$，则 $f(x)$ 不可约.

提示：证明 $f(x)$ 无重根.

(ii) 设 E/k 是有限扩张. 证明 E/k 是 $k[x]$ 中的某个多项式的分裂域，当且仅当每一个在 E 中有一个根的不可约多项式 $p(x) \in k[x]$ 在 $E[x]$ 中是分裂的.（比较使用了可分性假设的定理 4.34.）

4.12 (i) 证明：如果 σ 是 5-轮换，τ 是对换，则 S_5 由 $\{\sigma, \tau\}$ 生成.

提示：用习题2.94(iii).

(ii) 举出一个例子说明对于某个 n，S_n 包含一个 n-轮换 σ 和一个对换 τ 使得 $\langle\sigma, \tau\rangle \neq S_n$.

4.13 设 $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$，并设 G 是它的伽罗瓦群.

(i) 假定 $f(x)$ 是不可约多项式，证明 $|G|$ 是 5 的倍数. [可以用定理 6.34 即艾森斯坦 (Eisenstein) 准则证明 $f(x)$ 是不可约的.]

(ii) 证明 $f(x)$ 有三个实根和两个复根，当然两个复根是共轭的. 由此推出，如果把 $f(x)$ 的伽罗瓦群

G 看作 S_5 的子群，则 G 包含复共轭，它是 $f(x)$ 的根的一个对换.

（ⅲ）证明 $G \cong S_5$，由此推出 $f(x)$不是运用根式可解的.

提示：用习题 4.12.

4.2 伽罗瓦理论的基本定理

伽罗瓦理论分析了域 k 的代数扩张 E 和相应的伽罗瓦群 $\mathrm{Gal}(E/k)$ 之间的联系，这种联系使我们能够证明伽罗瓦定理的逆定理：如果 k 是特征 0 的域，且 $f(x) \in k[x]$ 有可解的伽罗瓦群，则 $f(x)$ 是运用根式可解的. 代数基本定理也是这种分析的推论.

我们已经看到几个关于伽罗瓦群的定理，这些定理的假设都涉及成为某个多项式的分裂域的扩张. 我们从下面的问题开始：是否存在扩张 E/k 的某种内在的性质可以刻画这种形成分裂域的扩张，而不涉及 $k[x]$ 中的任何特定的多项式. 由此产生了了解分裂域 E/k 的一种方法，就是在可分性和伽罗瓦群在 E 上的作用这两个环境中考察它们.

设 E 是域，$\mathrm{Aut}(E)$ 是 E 上一切（域）自同构形成的群. 如果 k 是 E 的任一子域，则 $\mathrm{Gal}(E/k)$ 是 $\mathrm{Aut}(E)$ 的子群，因而作用在 E 上. 只要有群作用在集合上，我们感兴趣的便是它的轨道和稳定化子，但现在要求被 $\mathrm{Aut}(E)$ 的某个子集 H 中的每个 σ 稳定的那些 E 的元素.

定义 如果 E 是域且 H 是 $\mathrm{Aut}(E)$ 的子集，则定义 H 的**固定域**为

218

$$E^H = \{a \in E: 对一切\ \sigma \in H, \sigma(a) = a\}.$$

固定域 E^H 的最重要的实例是当 H 是 $\mathrm{Aut}(E)$ 的子群时形成的，但也会遇到 H 仅仅是一个子集的情形.

易知，如果 $\sigma \in \mathrm{Aut}(E)$，则 $E^\sigma = \{a \in E : \sigma(a) = a\}$ 是 E 的子域；因为

$$E^H = \bigcap_{\sigma \in H} E^\sigma,$$

从而 E^H 是 E 的子域.

在例 3.125 中，我们考虑了 $E = k(y_1, \cdots, y_n)$，它是系数在域 k 中的 n 个变量的有理函数域，也考虑了 E 的子域 $K = k(a_0, \cdots, a_{n-1})$，其中

$$f(x) = (x - y_1)(x - y_2)\cdots(x - y_n) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$$

是 k 上的 n 次一般多项式. 因为 E 是添加 $f(x)$ 的一切根，也就是一切 y 到 K 形成的，从而知道 E 是 $f(x)$ 在 K 上的分裂域. 由于 $y_1, \cdots, y_n$ 的每个置换可以扩张成 E 的一个自同构，所以对称群 $S_n \leqslant \mathrm{Aut}(E)$，于是 $K = E^{S_n}$. 常称 K 的元素为 k 上 n 个变量的对称函数.

定义 有理函数 $g(x_1, \cdots, x_n)/h(x_1, \cdots, x_n) \in k(x_1, \cdots, x_n)$ 称为**对称函数**，如果置换它的变量保持函数不变：对每个 $\sigma \in S_n$，有 $g(x_{\sigma 1}, \cdots, x_{\sigma n})/h(x_{\sigma 1}, \cdots, x_{\sigma n}) = g(x_1, \cdots, x_n)/h(x_1, \cdots, x_n)$.

198 页等式（1）中的各个多项式定义了对称函数的样本，它们叫做**初等对称函数**.

下一命题的证明几乎是显然的.

命题 4.28 设 E 是域，则从 $\mathrm{Aut}(E)$ 的子集 H 到 E 的子域的函数 $H \mapsto E^H$ 是**反序**的：如果 $H \leqslant L \leqslant \mathrm{Aut}(E)$，则 $E^L \subseteq E^H$.

证明 如果 $a \in E^L$，则对一切 $\sigma \in L, \sigma(a) = a$. 因 $H \leqslant L$，从而对一切 $\sigma \in H, \sigma(a) = a$. 因此 $E^L \subseteq E^H$. ■

例 4.29 假设 k 是 E 的子域且 $G = \mathrm{Gal}(E/k)$. 显然 $k \subseteq E^G$，但包含关系可以是严格的. 例如，设 $E = \mathbb{Q}(\sqrt[3]{2})$，如果 $\sigma \in G = \mathrm{Gal}(E/\mathbb{Q})$，则 σ 必定固定 $\mathbb{Q}$，从而它置换 $f(x) = x^3 - 2$ 的根. 但

$f(x)$ 的另外两个根不是实数，所以 $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. 根据引理 4.2，$\sigma$ 是恒等函数，即 $E^G=E$. 注意 E 不是 $f(x)$ 的分裂域. ■

我们紧接着的目标是确定次数 $[E:E^G]$，其中 $G \leqslant \mathrm{Aut}(E)$. 为此，引入特征标的概念. [219]

定义 群 G 在域 E 中的**特征标**[⊖]是指（群）同态 $\sigma: G \to E^\times$，其中 $E^\times$ 是域 E 的非零元素的乘法群.

如果 $\sigma \in \mathrm{Aut}(E)$，则它的限制 $\sigma \mid E^\times: E^\times \to E^\times$ 是 E 中的一个特征标.

定义 如果 E 是域且 $G \leqslant \mathrm{Aut}(E)$，则 G 在 E 中的特征标的一个表 $\sigma_1, \cdots, \sigma_n$ 称为**无关的**，如果对于任意的 $c_1, \cdots, c_n \in E$，且

$$\text{对一切 } x \in G \text{ 有} \quad \sum_i c_i \sigma_i(x) = 0,$$

则一切 $c_i = 0$.

在例3.82(ⅲ)中，我们看到从集合 X 到域 E 的一切函数的集合 E^X 是 E 上的向量空间，其中函数的加法定义为

$$\sigma + \tau: x \mapsto \sigma(x) + \tau(x),$$

对 $c \in E$，标量乘法定义为

$$c\sigma: x \mapsto c\sigma(x).$$

当 X 是群 G 时，刚才定义的特征标的无关性就是向量空间 E^X 中的线性无关性.

命题 4.30（戴得金） 群 G 在域 E 中的不同特征标的每个表 $\sigma_1, \cdots, \sigma_n$ 都是无关的.

证明 对 $n \geqslant 1$ 用归纳法. 基础步 $n=1$ 成立，这是因为对一切 $x \in G$，如果 $c\sigma(x) = 0$，则不是 $c=0$ 就是 $\sigma(x) = 0$，但因 $\mathrm{im}\sigma \subseteq E^\times$，所以 $\sigma(x) \neq 0$.

假定 $n>1$，如果特征标不是无关的，则存在不全为零的 $c_i \in E$ 使得对一切 $x \in G$，

$$c_1\sigma_1(x) + \cdots + c_{n-1}\sigma_{n-1}(x) + c_n\sigma_n(x) = 0. \tag{2}$$

可以假定一切 $c_i \neq 0$，否则可以调用归纳假设而得出所需的矛盾. 如有必要则乘以 c_n^{-1}，从而可以假定 $c_n = 1$. 因 $\sigma_n \neq \sigma_1$，存在 $y \in G$ 使得 $\sigma_1(y) \neq \sigma_n(y)$. 在等式 (2) 中用 yx 替换 x，因 $\sigma_i(yx) = \sigma_i(y)\sigma_i(x)$，得

$$c_1\sigma_1(y)\sigma_1(x) + \cdots + c_{n-1}\sigma_{n-1}(y)\sigma_{n-1}(x) + \sigma_n(y)\sigma_n(x) = 0,$$ [220]

现在该等式乘以 $\sigma_n(y)^{-1}$ 得等式

$$c_1\sigma_n(y)^{-1}\sigma_1(y)\sigma_1(x) + \cdots + c_{n-1}\sigma_n(y)^{-1}\sigma_{n-1}(y)\sigma_{n-1}(x) + \sigma_n(x) = 0.$$

从等式 (2) 中减去上面的等式得 $n-1$ 项的和：

$$c_1[1 - \sigma_n(y)^{-1}\sigma_1(y)]\sigma_1(x) + c_2[1 - \sigma_n(y)^{-1}\sigma_2(y)]\sigma_2(x) + \cdots = 0.$$

由归纳假设，每个系数 $c_i[1 - \sigma_n(y)^{-1}\sigma_i(y)] = 0$. 因 $c_i \neq 0$，从而对一切 $i<n$ 有 $\sigma_n(y)^{-1}\sigma_i(y) = 1$，特别地，$\sigma_n(y) = \sigma_1(y)$，与 y 的定义矛盾. ■

引理 4.31 如果 $G = \{\sigma_1, \cdots, \sigma_n\}$ 是域 E 上 n 个不同自同构的集合，则

$$[E:E^G] \geqslant n.$$

证明 假定 $[E:E^G]=r<n$，并设 $\alpha_1, \cdots, \alpha_r$ 是 E/E^G 的基. 考虑 E 上 n 个未知数 r 个方程

⊖ 这个定义是表示论中的特征标的一个特殊情形：如果 $\sigma: G \to \mathrm{GL}(n,E)$ 是同态，则它的特征标 $\chi_\sigma: G \to E$ 定义为对 $x \in G$，

$$\chi_\sigma(x) = \mathrm{trace}(\sigma(x)),$$

其中 $n \times n$ 矩阵的迹（trace）是其对角线元素的和. 当 $n=1$ 时，$\mathrm{GL}(1,E) = E^\times$，且称 $\chi_\sigma(x) = \sigma(x)$ 为**线性特征标**.

的齐次线性方程组：

$$\sigma_1(\alpha_1)x_1+\cdots+\sigma_n(\alpha_1)x_n=0$$
$$\sigma_1(\alpha_2)x_1+\cdots+\sigma_n(\alpha_2)x_n=0$$
$$\vdots$$
$$\sigma_1(\alpha_r)x_1+\cdots+\sigma_n(\alpha_r)x_n=0.$$

因 $r<n$，方程数小于变量个数，从而在 E^n 中有非平凡解 $(c_1,\cdots,c_n)$.

现在要证明对任意 $\beta\in E^\times$，$\sigma_1(\beta)c_1+\cdots+\sigma_n(\beta)c_n=0$，它与特征标 $\sigma_1\mid E^\times,\cdots,\sigma_n\mid E^\times$ 的无关性相矛盾. 因 $\alpha_1,\cdots,\alpha_r$ 是 E 在 E^G 上的基，每个 $\beta\in E$ 可以写作

$$\beta=\sum b_i\alpha_i,$$

其中 $b_i\in E^G$. 方程组的第 i 行乘以 $\sigma_1(b_i)$ 得第 i 行为

$$\sigma_1(b_i)\sigma_1(\alpha_i)c_1+\cdots+\sigma_1(b_i)\sigma_n(\alpha_i)c_n=0$$

的方程组. 但因 $b_i\in E^G$，对一切 i,j，$\sigma_1(b_i)=b_i=\sigma_j(b_i)$，于是方程组的第 i 行成为

$$\sigma_1(b_i\alpha_i)c_1+\cdots+\sigma_n(b_i\alpha_i)c_n=0.$$

把一切行加起来得到

$$\sigma_1(\beta)c_1+\cdots+\sigma_n(\beta)c_n=0,$$

221 与特征标 $\sigma_1,\cdots,\sigma_n$ 的无关性矛盾. ■

命题 4.32 如果 $G=\{\sigma_1,\cdots,\sigma_n\}$ 是 $\mathrm{Aut}(E)$ 的子群，则

$$[E:E^G]=|G|.$$

证明 根据引理 4.31，只需证明 $[E:E^G]\leqslant|G|$. 如果 $[E:E^G]>n$，设 $\{\omega_1,\cdots,\omega_{n+1}\}$ 是 E^G 上的向量空间 E 中的线性无关向量表. 考虑有 $n+1$ 个未知数 n 个方程的方程组：

$$\sigma_1(\omega_1)x_1+\cdots+\sigma_1(\omega_{n+1})x_{n+1}=0$$
$$\vdots$$
$$\sigma_n(\omega_1)x_1+\cdots+\sigma_n(\omega_{n+1})x_{n+1}=0.$$

在 E 上有非平凡解 $(\alpha_1,\cdots,\alpha_{n+1})$，我们进一步把它正规化. 选取非零分量个数 r 最少的一个解 $(\beta_1,\cdots,\beta_r,0,\cdots,0)$（对 ω_i 重新标号，可以假定非零分量出现最在前面）. 注意 $r\neq1$，以免 $\sigma_1(\omega_1)\beta_1=0$ 蕴涵 $\beta_1=0$. 如有必要乘以 β_r 的逆，从而可以假定 $\beta_r=1$. 并非所有的 $\beta_i\in E^G$，以免对应于 $\sigma=1_E$ 的行违背 $\{\omega_1,\cdots,\omega_{n+1}\}$ 的线性无关性. 最后一个假设是 β_1 不在 E^G 中（也可以用重新标号 ω_i 的方法完成）. 于是存在 σ_k 使得 $\sigma_k(\beta_1)\neq\beta_1$. 因 $\beta_r=1$，原始方程组的第 j 行为

$$\sigma_j(\omega_1)\beta_1+\cdots+\sigma_j(\omega_{r-1})\beta_{r-1}+\sigma_j(\omega_r)=0. \tag{3}$$

把 σ_k 作用到这个方程组上得

$$\sigma_k\sigma_j(\omega_1)\sigma_k(\beta_1)+\cdots+\sigma_k\sigma_j(\omega_{r-1})\sigma_k(\beta_{r-1})+\sigma_k\sigma_j(\omega_r)=0.$$

因 G 是群，$\sigma_k\sigma_1,\cdots,\sigma_k\sigma_n$ 恰好是 $\sigma_1,\cdots,\sigma_n$ 的置换. 设 $\sigma_k\sigma_j=\sigma_i$，方程组的第 i 行为

$$\sigma_i(\omega_1)\sigma_k(\beta_1)+\cdots+\sigma_i(\omega_{r-1})\sigma_k(\beta_{r-1})+\sigma_i(\omega_r)=0.$$

从方程 (3) 的第 i 行减去这一行，得新的方程组的第 i 行为

$$\sigma_i(\omega_1)[\beta_1-\sigma_k(\beta_1)]+\cdots+\sigma_i(\omega_{r-1})[\beta_{r-1}-\sigma_k(\beta_{r-1})]=0.$$

因 $\beta_1-\sigma_k(\beta_1)\neq0$，我们便找到原始方程组的一个非平凡解，其非零分量的个数少于 r，于是得出矛盾. ■

这些思想给出伽罗瓦理论的基本定理的证明中需要的一个结果.

定理 4.33 如果 G 和 H 是 $\mathrm{Aut}(E)$ 的有限子群且满足 $E^G=E^H$，则 $G=H$.

证明 首先证明如果 $\sigma\in\mathrm{Aut}(E)$，则 σ 固定 E^G 当且仅当 $\sigma\in G$. 显然，如果 $\sigma\in G$，则 σ 固定 E^G. 反之，假定 σ 固定 E^G 而 $\sigma\notin G$. 如果 $|G|=n$，则根据命题 4.32，

222

$$n=|G|=[E:E^G].$$

因 σ 固定 E^G，所以有 $E^G\subseteq E^{G\cup\{\sigma\}}$，但根据命题 4.28，反过来的不等式恒成立，所以 $E^G=E^{G\cup\{\sigma\}}$. 因此由引理 4.31，

$$n=[E:E^G]=[E:E^{G\cup\{\sigma\}}]\geqslant|G\cup\{\sigma\}|=n+1,$$

得出矛盾 $n\geqslant n+1$.

如果 $\sigma\in H$，则 σ 固定 $E^H=E^G$，因此 $\sigma\in G$；即 $H\leqslant G$. 用同样的方法可以证明反过来的包含关系成立，所以 $H=G$. ■

现在可以给出我们一直所寻找的分裂域的刻画.

定理 4.34 如果 E/k 是有限扩张，它具有伽罗瓦群 $G=\mathrm{Gal}(E/k)$，则下列陈述等价：

(i) E 是某个可分多项式 $f(x)\in k[x]$ 的分裂域.

(ii) $k=E^G$.

(iii) 每个有根在 E 中的不可约多项式 $p(x)\in k[x]$ 在 $E[x]$ 中是可分的和分裂的.

证明 (i) ⇒ (ii). 由定理 4.7 (ii)，$|G|=[E:k]$. 但命题 4.32 给出 $|G|=[E:E^G]$，所以

$$[E:k]=[E:E^G].$$

因 $k\leqslant E^G$，因而有 $[E:k]=[E:E^G][E^G:k]$，从而 $[E^G:k]=1$ 且 $k=E^G$.

(ii) ⇒ (iii). 设 $p(x)\in k[x]$ 是以 E 中的 α 为根的不可约多项式，并设集合 $\{\sigma(\alpha):\sigma\in G\}$ 的不同元素是 $\alpha_1,\cdots,\alpha_n$. 定义 $g(x)\in E[x]$ 为

$$g(x)=\prod(x-\alpha_i).$$

现在每个 $\sigma\in G$ 置换 α_i，从而每个 σ 固定 $g(x)$ 的系数；即 $g(x)$ 的系数在 $E^G=k$ 中. 因此 $g(x)$ 是 $k[x]$ 中无重根的多项式. 现在 $p(x)$ 和 $g(x)$ 在 E 中有一个公共根，从而它们在 $E[x]$ 中的 gcd 不是 1，根据系 3.41，它们在 $k[x]$ 中的 gcd 也不是 1. 因 $p(x)$ 不可约，它必整除 $g(x)$. 所以 $p(x)$ 无重根，因而是可分的，且在 E 上分裂.

(iii) ⇒ (i). 选取 $\alpha_1\in E$ 且 $\alpha_1\notin k$. 因 E/k 是有限扩张，α_1 必是 k 上的代数元素. 设 $p_1(x)=\mathrm{irr}(\alpha_1,k)\in k[x]$ 是 α_1 的极小多项式. 根据假设，$p_1(x)$ 是可分多项式且在 E 上分裂. 令 $K_1\subseteq E$ 是它的分裂域. 如果 $K_1=E$，证明已经完成. 否则，选取 $\alpha_2\in E$ 且 $\alpha_2\notin K_1$. 根据假设，存在可分不可约多项式 $p_2(x)\in k[x]$ 以 α_2 为根. 令 $K_2\subseteq E$ 是可分多项式 $p_1(x)p_2(x)$ 的分裂域. 如果 $K_2=E$，则证明完成，否则重复这一构造. 因为 E/k 是有限的，该过程必定要终止，即有某个 m 使得 $K_m=E$. 于是 E 是可分多项式 $p_1(x)\cdots p_m(x)$ 的分裂域. ■

223

定义 域扩张 E/k 称为**伽罗瓦扩张**，如果它满足定理 4.34 中任何一个等价条件.

例 4.35 如果 E/k 是有限可分扩张，则引理 4.17 中构造的 E 的根式扩张是伽罗瓦扩张. ■

系 4.36 如果 E/k 是伽罗瓦扩张，B 是一个**中间域**，即子域 B 满足 $k\subseteq B\subseteq E$，则 E/B 是伽罗瓦扩张.

证明 我们知道 E 是某个可分多项式 $f(x)\in k[x]$ 的分裂域；即 $E=k(\alpha_1,\cdots,\alpha_n)$，其中 $\alpha_1,\cdots,\alpha_n$ 是 $f(x)$ 的根. 因 $k\subseteq B\subseteq E$，有 $f(x)\in B[x]$ 且 $E=B(\alpha_1,\cdots,\alpha_n)$. ■

回忆 n 个变量的初等对称函数是多项式

$$e_j(x_1,\cdots,x_n)=\sum_{i_1<\cdots<i_j} x_{i_1}\cdots x_{i_j},$$

其中 $j=1,\cdots,n$.

如果 $z_1,\cdots,z_n$ 是 $x^n+a_{n-1}x^{n-1}+\cdots+a_0$ 的根，则 $e_j(z_1,\cdots,z_n)=(-1)^j a_{n-j}$.

定理 4.37 (对称函数的基本定理) 如果 k 是域，则 $k(x_1,\cdots,x_n)$ 中的每个对称函数都是初等对称函数 $e_1,\cdots,e_n$ 中的有理函数.

证明 设 F 是 $E=k(x_1,\cdots,x_n)$ 的包含 k 和初等对称函数的最小子域. 如同我们在例 3.125 中看到的那样，E 是 n 次一般多项式 $f(t)$ 的分裂域，其中

$$f(t)=\prod_{i=1}^{n}(t-x_i).$$

因 $f(t)$ 是可分多项式，所以 E/F 是伽罗瓦扩张. 在阿贝尔-鲁菲尼定理(即定理4.27)的证明中，我们知道 $\mathrm{Gal}(E/F)\cong S_n$，所以由定理 4.34，$E^{S_n}=F$. 但是说 $\theta(x)=g(x_1,\cdots,x_n)/h(x_1,\cdots,x_n)$ 在 E^{S_n} 中就是说它在变量的置换下不变；即 $\theta(x)$ 是对称函数. ■

习题 6.84 证明 $k[x_1,\cdots,x_n]$ 中的每个对称多项式都在 $k[e_1,\cdots,e_n]$ 中.

定义 设 A 和 B 是域 E 的子域，则它们的**复合域**是指 E 的一切包含 $A\cup B$ 的子域的交，记为 $A\vee B$.

易知 $A\vee B$ 是 E 的包含 A 和 B 的最小子域. 例如，如果 E/k 是一个扩张具有中间域 $A=k(\alpha_1,\cdots,\alpha_n)$ 和 $B=k(\beta_1,\cdots,\beta_m)$，则它们的复合域是

224

$$k(\alpha_1,\cdots,\alpha_n)\vee k(\beta_1,\cdots,\beta_m)=k(\alpha_1,\cdots,\alpha_n,\beta_1,\cdots,\beta_m).$$

命题 4.38 (ⅰ) 每个伽罗瓦扩张 E/k 都是 k 的分裂扩张.

(ⅱ) 如果 E/k 是代数域扩张且 $S\subseteq E$ 是任意一个可分元素的集合，它可以是无限的[⊖]，则 $k(S)/k$ 是可分扩张.

(ⅲ) 设 E/k 是代数扩张，其中 k 是域，且 B 和 C 是中间域. 如果 B/k 和 C/k 都是可分扩张，则它们的复合域 $B\vee C$ 也是 k 的可分扩张.

证明 (ⅰ) 如果 $\beta\in E$，则 $p(x)=\mathrm{irr}(\beta,k)\in k[x]$ 是 $k[x]$ 中有一个根在 E 中的不可约多项式. 由定理4.34(ⅲ)，$p(x)$ 是可分多项式（它在 $E[x]$ 中分裂）. 所以 β 在 k 上可分，从而 E/k 是可分扩张.

(ⅱ) 先考虑 S 有限的情形，即 $B=k(\alpha_1,\cdots,\alpha_t)$ 是有限扩张，其中每个 α_i 在 k 上是可分的. 根据引理4.17(ⅰ)，存在扩张 E/B，它是某个可分多项式 $f(x)\in k[x]$ 的分裂域，因此根据定理4.34(ⅰ)，E/k 是伽罗瓦扩张. 根据本命题的（ⅰ），E/k 是可分扩张，即对于一切 $\alpha\in E$，多项式 $\mathrm{irr}(\alpha,k)$ 无重根. 特别地，对于一切 $\alpha\in B$，$\mathrm{irr}(\alpha,k)$ 无重根，因此 B/k 是可分扩张.

现在考虑一般情形. 如果 $\alpha\in k(S)$，则习题 3.95 说存在有限个元素 $\alpha_1,\cdots,\alpha_n\in S$ 使得 $\alpha\in B=k(\alpha_1,\cdots,\alpha_n)$. 因为刚才我们已知 B/k 是可分扩张，从而 α 在 k 上是可分的. 因为 α 是 $k(S)$ 的任意元素，从而 $k(S)/k$ 是可分扩张.

(ⅲ) 因为 $B\vee C=k(B\cup C)$，把（ⅰ）运用到子集 $S=B\cup C$ 即可. ■

⊖ 如果添加有限多个超越元素则该结果成立（回忆可分的定义，超越元素恒为可分元素），但如果添加无限多个超越元素则结果可能不成立.

问题 如果 E/k 是伽罗瓦扩张且 B 是中间域，那么 B/k 是伽罗瓦扩张吗？答案是否定的. 在例 4.29 中，我们看到 $E=\mathbb{Q}(\sqrt[3]{2},\omega)$ 是$\mathbb{Q}$上的多项式 x^3-2 的分裂域，其中 ω 是三次单位原根，因此它是伽罗瓦扩张. 然而，中间域 $B=\mathbb{Q}(\sqrt[3]{2})$ 不是伽罗瓦扩张，因为 x^3-2 是有根在 B 中的不可约多项式，但它在 $B[x]$ 中不分裂.

下面的命题判定中间域 B 在什么时候是伽罗瓦扩张.

定义 如果 E/k 是伽罗瓦扩张，B 是中间域，则对于某个 $\sigma\in\mathrm{Gal}(E/k)$，中间域

$$B^{\sigma}=\{\sigma(b):b\in B\}$$

称为 B 的一个**共轭**.

225

命题 4.39 如果 E/k 是伽罗瓦扩张，则中间域 B 除了 B 自身之外没有其他的共轭当且仅当B/k 是伽罗瓦扩张.

证明 假定对一切 $\sigma\in G, B^{\sigma}=B$,其中 $G=\mathrm{Gal}(E/k)$. 设不可约多项式 $p(x)\in k[x]$ 在 B 中有根 β，因 $B\subseteq E$ 且 E/k 是伽罗瓦扩张，所以 $p(x)$ 是可分多项式且在 $E[x]$ 中分裂. 如果 $\beta'\in E$ 是 $p(x)$ 的另一个根，则存在同构 $\sigma\in G$ 使得 $\sigma(\beta)=\beta'$（因为根据命题 4.13，G 传递地作用在不可约多项式的根上)，因此 $\beta'=\sigma(\beta)\in B^{\sigma}=B$，从而 $p(x)$ 在 $B[x]$ 中分裂，所以 B/k 是伽罗瓦扩张.

反之，因 B/k 是k 上某个多项式 $f(x)$ 的分裂域，所以 $B=k(\alpha_1,\cdots,\alpha_n)$，其中 $\alpha_1,\cdots,\alpha_n$ 是 $f(x)$ 所有的根. 因每个 $\sigma\in\mathrm{Gal}(E/k)$ 必置换 $f(x)$ 的根，从而 σ 必把 B 发送到它自身. ■

现在证明当 E/k 是伽罗瓦扩张的时候，中间域被 $\mathrm{Gal}(E/k)$ 的子群分类.

我们从几个一般性定义开始.

定义 集合 X 称为**偏序集**，如果其上定义了一个二元关系 $x\preceq y$，对一切 $x,y,z\in X$ 满足

(i) **自反性**：$x\preceq x$;

(ii) **反对称性**：如果 $x\preceq y$ 且 $y\preceq x$，则 $x=y$;

(iii) **传递性**：如果 $x\preceq y$ 且 $y\preceq z$，则 $x\preceq z$.

偏序集 X 中的元素 c 称为a，$b\in X$ 的**上界**，如果 $a\preceq c$ 且 $b\preceq c$. 元素 $d\in X$ 称为a，b 的**最小上界**，如果 d 是上界且对 a，b 的每个上界 c 有 $d\preceq c$. 把不等号反转，可类似地定义**下界**和**最大下界**.

在附录中更彻底地讨论了偏序集，这里我们更关注的是称为格的特殊偏序集.

定义 **格**是指偏序集$\mathcal{L}$，其中每对元素 $a,b\in\mathcal{L}$ 都有最大下界 $a\wedge b$ 和最小上界 $a\vee b$.

例 4.40 (i) 如果 U 是一个集合，定义$\mathcal{L}$为 U 的全体子集的族，且定义 $A\preceq B$ 表示 $A\subseteq B$，则$\mathcal{L}$是格，其中 $A\wedge B=A\cap B, A\vee B=A\cup B$.

(ii) 如果 G 是一个群，定义 $\mathcal{L}=\mathrm{Sub}(G)$ 为 G 的一切子群的族，且定义 $A\preceq B$ 表示 $A\leqslant B$，即 A 是 B 的子群，则$\mathcal{L}$是格，其中 $A\wedge B=A\cap B, A\vee B$ 是$A\cup B$ 生成的子群.

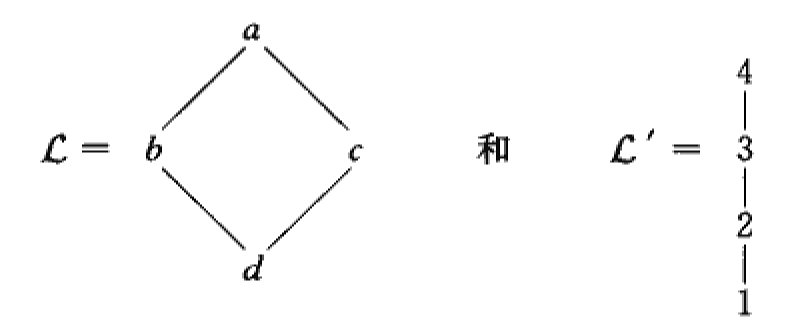
(iii) 如果 E/k 是域扩张，定义 $\mathcal{L}=\mathrm{Int}(E/k)$ 为一切中间域的族，且定义 $K\preceq B$ 表示 $K\subseteq B$，即 K 是 B 的子域，则$\mathcal{L}$是格，其中 $K\wedge B=K\cap B, K\vee B$ 是 K 和 B 的复合域.

226

(iv) 如果 n 是正整数，定义 $\mathrm{Div}(n)$ 为 n 的全体正因数的集合. 如果定义 $d\preceq d'$ 表示 $d\mid d'$,则 $\mathrm{Div}(n)$ 是偏序集. 这里 $d\wedge d'=\gcd(d,d'), d\vee d'=\mathrm{lcm}(d,d')$. ■

定义 如果$\mathcal{L}$和$\mathcal{L}'$是格，函数 $f:\mathcal{L}\to\mathcal{L}'$ 称为**反序的**,如果在$\mathcal{L}$中有 $a\preceq b$ 蕴涵在$\mathcal{L}'$中有 $f(b)\preceq f(a)$.

例 4.41 存在格$\mathcal{L}$和$\mathcal{L}'$以及反序的双射$\varphi:\mathcal{L}\to\mathcal{L}'$,它的逆$\varphi^{-1}:\mathcal{L}'\to\mathcal{L}$不是反序的. 例如考虑格



定义双射 $\varphi:\mathcal{L}\to\mathcal{L}'$ 为

$$\varphi(a)=1,\varphi(b)=2,\varphi(c)=3,\varphi(d)=4,$$

这是一个反序双射，但它的逆 $\varphi^{-1}:\mathcal{L}'\to\mathcal{L}$ 不是反序的，因为 $2\leq 3$ 但 $c=\varphi^{-1}(3)\npreceq\varphi^{-1}(2)=b$. ■

德摩根定律说，如果 A 和 B 是集合 X 的子集，且 A' 表示 A 的补集，则

$$(A\cap B)'=A'\cup B',(A\cup B)'=A'\cap B'.$$

下面的引理推广了这两个恒等式.

引理 4.42 设$\mathcal{L}$和$\mathcal{L}'$是格，$\varphi:\mathcal{L}\to\mathcal{L}'$是使得 φ 和 φ^{-1} 都是反序的双射，则

$$\varphi(a\wedge b)=\varphi(a)\vee\varphi(b),\varphi(a\vee b)=\varphi(a)\wedge\varphi(b).$$

证明 因 $a,b\leq a\vee b$,所以有 $\varphi(a\vee b)\leq\varphi(a),\varphi(b)$,即 $\varphi(a\vee b)$ 是 $\varphi(a),\varphi(b)$ 的下界，从而 $\varphi(a\vee b)\leq\varphi(a)\wedge\varphi(b)$.

关于反过来的不等式，φ 的满射性给出 $c\in\mathcal{L}$使得 $\varphi(a)\wedge\varphi(b)=\varphi(c)$. 现在 $\varphi(c)=\varphi(a)\wedge\varphi(b)\leq\varphi(a),\varphi(b)$. φ^{-1} 也是反序的，把 φ^{-1} 作用上去，有 $a,b\leq c$. 因此 c 是 a,b 的上界，从而 $a\vee b\leq c$. 所以 $\varphi(a\vee b)\geq\varphi(c)=\varphi(a)\wedge\varphi(b)$. 类似的论证可得命题的另一半. ■

227

定理 4.43（伽罗瓦理论的基本定理） 设 E/k 是有限伽罗瓦扩张，它具有伽罗瓦群 $G=\mathrm{Gal}(E/k)$.

（i）定义函数 $\gamma:\mathrm{Sub}(\mathrm{Gal}(E/k))\to\mathrm{Int}(E/k)$ 为

$$\gamma: H\mapsto E^H,$$

则 γ 是反序双射，它的逆 $\delta:\mathrm{Int}(E/k)\to\mathrm{Sub}(\mathrm{Gal}(E/k))$ 是反序双射

$$\delta: B\mapsto\mathrm{Gal}(E/B).$$

（ii）对每个 $B\in\mathrm{Int}(E/k)$ 和 $H\in\mathrm{Sub}(\mathrm{Gal}(E/k))$,

$$E^{\mathrm{Gal}(E/B)}=B\quad\text{且}\ \mathrm{Gal}(E/E^H)=H.$$

（iii）对每个 $H,K\in\mathrm{Sub}(\mathrm{Gal}(E/k))$ 和 $B,C\in\mathrm{Int}(E/k)$,

$$E^{H\vee K}=E^H\cap E^K;$$
$$E^{H\cap K}=E^H\vee E^K;$$
$$\mathrm{Gal}(E/(B\vee C))=\mathrm{Gal}(E/B)\cap\mathrm{Gal}(E/C);$$
$$\mathrm{Gal}(E/(B\cap C))=\mathrm{Gal}(E/B)\vee\mathrm{Gal}(E/C).$$

（iv）对每个 $B\in\mathrm{Int}(E/k)$ 和 $H\in\mathrm{Sub}(\mathrm{Gal}(E/k))$,

$$[B:k]=[G:\mathrm{Gal}(E/B)]\quad\text{且}[G:H]=[E^H:k].$$

（v）如果 $B\in\mathrm{Int}(E/k)$,则 B/k 是伽罗瓦扩张当且仅当 $\mathrm{Gal}(E/B)$ 是 G 的正规子群.

证明 （i）命题 4.28 证明 γ 是反序的，也容易证明 δ 是反序的. 现在定理 4.33 证明 γ 是单

射，从而根据命题 1.47，只需证明 $\gamma\delta$：$\text{Int}(E/k)\to\text{Int}(E/k)$ 是恒等函数，由此可导出 γ 是具有逆 δ 的双射. 如果 B 是一个中间域，则 $\gamma\delta$：$B\mapsto E^{\text{Gal}(E/B)}$. 但根据系 4.36，$E/E^B$ 是伽罗瓦扩张，从而根据定理 4.34，$E^{\text{Gal}(E/B)}=B$.

（ⅱ）该结果就是说 $\gamma\delta$ 和 $\delta\gamma$ 是恒等函数.

（ⅲ）从引理 4.42 可得.

（ⅳ）根据定理4.7（ⅱ）和 E/B 是伽罗瓦扩张的事实，

$$[B:k]=[E:k]/[E:B]=|G|/|\text{Gal}(E/B)|=[G:\text{Gal}(E/B)].$$

由此 B/k 的次数是它的伽罗瓦群在 G 中的指数. 第二个等式也由该式导出，只要取 $B=E^H$，注意到（ⅱ）给出 $\text{Gal}(E/E^H)=H$：

$$[E^H:k]=[G:\text{Gal}(E/E^H)]=[G:H].$$

228

（ⅴ）由定理 4.16，当 B/k 是伽罗瓦扩张时，$\text{Gal}(E/B)\lhd G$(B/k 和 E/k 都是 $k[x]$ 中多项式的分裂域). 关于逆命题，设 $H=\text{Gal}(E/B)$，并假定 $H\lhd G$. 现在根据（ⅱ），$E^H=E^{\text{Gal}(E/B)}=B$，从而根据命题 4.39 只需证明对每个 $\sigma\in G$，$(E^H)^\sigma=E^H$. 现在假设 $a\in E^H$，即对一切 $\eta\in H$，$\eta(a)=a$. 如果 $\sigma\in G$，则需要证明对一切 $\eta\in H$，$\eta(\sigma(a))=\sigma(a)$. 现在 $H\lhd G$ 说明如果 $\eta\in H$ 且 $\sigma\in G$，则存在 $\eta'\in H$ 使得 $\eta\sigma=\sigma\eta'$（当然 $\eta'=\sigma^{-1}\eta\sigma$）. 但因为 $\eta'(a)=a$，所以有

$$\eta\sigma(a)=\sigma\eta'(a)=\sigma(a),$$

因此 $B/k=E^H/k$ 是伽罗瓦扩张. ■

下面是几个推论.

定理 4.44 如果 E/k 是伽罗瓦扩张且它的伽罗瓦群是阿贝尔群，则每个中间域都是伽罗瓦扩张.

证明 阿贝尔群的每个子群都是正规子群. ■

系 4.45 一个伽罗瓦扩张 E/k 只有有限个中间域.

证明 有限群 $\text{Gal}(E/k)$ 只有有限个子群. ■

定义 域扩张 E/k 称为**单扩张**，如果存在 $u\in E$ 使得 $E=k(u)$.

下面属于施泰尼茨（E. Steinitz）的定理刻画了单扩张.

定理 4.46（施泰尼茨） 有限扩张 E/k 是单扩张当且仅当它只有有限个中间域.

证明 假定 E/k 是单扩张，于是 $E=k(u)$. 令 $p(x)=\text{irr}(u,k)\in k[x]$ 是它的极小多项式，如果 B 是任意一个中间域，令

$$q(x)=\text{irr}(u,B)=b_0+b_1x+\cdots+b_{n-1}x^{n-1}+x^n\in B[x]$$

为 u 在 B 上的首一不可约多项式，并定义

$$B'=k(b_0,\cdots,b_{n-1})\subseteq B.$$

注意 $q(x)$是较小的域 B'上的不可约多项式. 现在

$$E=k(u)\subseteq B'(u)\subseteq B(u)\subseteq E,$$

从而 $B'(u)=E=B(u)$，因此$[E:B]=[B(u):B]$和$[E:B']=[B'(u):B']$. 但根据命题3.117（ⅴ），这每一个都等于 $\deg(q)$，从而$[E:B]=\deg(q)=[E:B']$. 因 $B'\subseteq B$，可以推出 $[B:B']=1$；即

$$B=B'=k(b_0,\cdots,b_{n-1}).$$

229

我们已经用 $q(x)$ 的系数刻画了 B，$q(x)$ 是 $p(x)=\text{irr}(u,k)$ 在 $E[x]$ 中的首一因式. 但 $p(x)$ 只有有限个首一因式，因此只有有限个中间域.

反之，假定 E/k 只有有限个中间域. 如果 k 是有限域，则我们知道 E/k 是一个单扩张（取 u 为本原元）. 所以可假定 k 是无限的. 因 E/k 是有限扩张，存在元素 $u_1,\cdots,u_n$ 使得 $E=k(u_1\cdots u_n)$. 对 $n\geqslant 1$ 用归纳法，只需证明 $E=k(a,b)$ 是单扩张. 现在因 k 是无限的，所以有无限个元素 $c\in E$ 形如 $c=a+tb$，其中 $t\in k$. 因为只有有限个中间域，特别是只有有限个形如 $k(c)$ 的域. 根据鸽笼原理[⊖]，存在不同的元素 $t,t'\in k$ 使得 $k(c)=k(c')$，其中 $c'=a+t'b$. 显然，$k(c)\subseteq k(a,b)$. 关于反包含，域 $k(c)=k(c')$ 包含 $c-c'=(t-t')b$，从而 $b\in k(c)$（因 $t-t'\neq 0$），由此 $a=c-tb\in k(c)$，所以 $k(c)=k(a,b)$. ■

可以立即得到的一个推论是每个伽罗瓦扩张都是单扩张，事实上还有更多的结论.

定理 4.47（本原元定理） 如果 B/k 是有限可分扩张，则存在 $u\in B$ 使得 $B=k(u)$. 特别地，如果 k 有特征 0，则每个有限扩张 B/k 都是单扩张.

证明 根据例 4.35，引理 4.17 中构造的根式扩张 E/k 是伽罗瓦扩张，它以 B 为一个中间域，从而根据系 4.45，扩张 E/k 只有有限个中间域，由此扩张 B/k 也只有有限个中间域，从而施泰尼茨定理表明 B/k 有本原元. ■

本原元定理由拉格朗日提出，伽罗瓦修改了这个定理以用于构造伽罗瓦群的原始形式.

现在回到有限域.

定理 4.48 有限域 $\mathbb{F}_q$（其中 $q=p^n$）对 n 的每个因数 d 恰有一个阶为 p^d 的子域，且再无其他子域.

证明 首先，因为 $\mathbb{F}_q/\mathbb{F}_p$ 是可分多项式 x^q-x 的分裂域，所以它是伽罗瓦扩张. 现在根据定理 4.12，$G=\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ 是 n 阶循环群. 由引理 2.85，对 n 的每个因数 d，n 阶循环群恰有一个 d 阶子群，从而 G 恰有一个指数为 n/d 的子群 H，所以只有一个中间域，它就是 E^H，满足 $[E^H:\mathbb{F}_p]=[G:H]=n/d$ 和 $E^H=\mathbb{F}_{p^{n/d}}$. ■

我们现在给出由高斯（1799）证明的代数基本定理的两种代数证明：第一个属于塞缪尔（P. Samuel）（他"运用了本质上属于拉格朗日的方法"），使用了对称函数的基本定理；第二个使用了伽罗瓦理论的基本定理以及将在第 5 章证明的西罗（Sylow）定理.

230

假定 $\mathbb{R}$ 满足弱形式的中值定理：如果 $f(x)\in\mathbb{R}[x]$，并存在 a，$b\in\mathbb{R}$ 使得 $f(a)>0$ 和 $f(b)<0$，则 $f(x)$ 有实根. 下面是一些初步推论.

（ⅰ）每个正实数 r 都有一个实平方根.

如果 $f(x)=x^2-r$，则

$$f(1+r)=(1+r)^2-r=1+r+r^2>0,$$

且 $f(0)=-r<0$.

（ⅱ）每个二次多项式 $g(x)\in\mathbb{C}[x]$ 都有一个复根.

首先，每个复数 z 都有一个复平方根：当 z 写成极坐标形式 $z=re^{i\theta}$ 时，其中 $r\geqslant 0$，则 $\sqrt{z}=\sqrt{r}e^{i\theta/2}$. 二次公式给出 $g(x)$ 的（复）根.

（ⅲ）域 $\mathbb{C}$ 没有 2 次扩张.

这样的扩张将包含这样的一个元素，它的极小多项式是 $\mathbb{C}[x]$ 中的二次不可约多项式，而（ⅱ）说明这样的多项式不存在.

（ⅳ）每个奇数次多项式 $f(x)\in\mathbb{R}[x]$ 都有实根.

⊖ 如果在有限个鸽笼中有无限只鸽子，则至少有一个鸽笼包含无限只鸽子.

设 $f(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}+x^n\in\mathbb{R}[x]$，定义 $t=1+\sum|a_i|$. 现在对一切 i，$|a_i|\leqslant t-1$，并且如果 $h(x)=f(x)-x^n$，则

$$\begin{aligned}|h(t)|&=|a_0+a_1t+\cdots+a_{n-1}t^{n-1}|\\&\leqslant(t-1)(1+t+\cdots+t^{n-1})\\&=t^n-1\\&<t^n.\end{aligned}$$

所以 $-t^n<h(t)$ 且 $0=-t^n+t^n<h(t)+t^n=f(t)$.

用类似的论证可以证明 $|h(-t)|<t^n$，从而

$$f(-t)=h(-t)+(-t)^n<t^n+(-t)^n.$$

当 n 是奇数时，$(-t)^n=-t^n$，从而 $f(-t)<t^n-t^n=0$，因此中值定理保证有实数 r 使得 $f(r)=0$；即 $f(x)$ 有实根.

（v）*不存在次数>1的奇数次域扩张 $E/\mathbb{R}$.*

如果 $u\in E$，则根据（iv），它的极小多项式 $\mathrm{irr}(u,\mathbb{R})$ 必是偶数次的，从而 $[\mathbb{R}(u):\mathbb{R}]$ 是偶数. 因此 $[E:\mathbb{R}]=[E:\mathbb{R}(u)][\mathbb{R}(u):\mathbb{R}]$ 是偶数.

231

定理 4.49（代数基本定理） *如果 $f(x)\in\mathbb{C}[x]$ 的次数 $n\geqslant1$，则 $f(x)$ 有复根，因此 $f(x)$ 分裂：存在 $c,u_1,\cdots,u_n\in\mathbb{C}$ 使得*

$$f(x)=c(x-u_1)\cdots(x-u_n).$$

证明 我们证明 $f(x)=\sum a_ix^i\in\mathbb{C}[x]$ 有复根. 定义 $\overline{f}(x)=\sum\overline{a}_ix^i$，其中 $\overline{a}_i$ 是 a_i 的复共轭. 现在 $f(x)\overline{f}(x)=\sum c_kx^k$，其中 $c_k=\sum\limits_{i+j=k}a_i\overline{a}_j$，因此 $\overline{c}_k=c_k$，从而 $f(x)\overline{f}(x)\in\mathbb{R}[x]$. 如果 $f(x)$ 有复根 z，则 z 是 $f(x)\overline{f}(x)$ 的根. 反之，如果 z 是 $f(x)\overline{f}(x)$ 的复根，则 z 或者是 $f(x)$ 的根，或者是 $\overline{f}(x)$ 的根. 而如果 z 是 $\overline{f}(x)$ 的根，则 $\overline{z}$ 是 $f(x)$ 的根，所以 $f(x)$ 有复根当且仅当 $f(x)\overline{f}(x)$ 有复根，因此只需证明每个实多项式有复根.

总之，只需证明每个非常数首一多项式 $f(x)\in\mathbb{R}[x]$ 有复根. 设 $\deg(f)=2^km$，其中 m 是奇数，对 $k\geqslant0$ 用归纳法证明该结果. 基础步 $k=0$ 已在（iv）中得证，从而可以假定 $k\geqslant1$. 设 $\alpha_1,\cdots,\alpha_n$ 是 $f(x)$ 在它的某个分裂域中的根，对于固定的 $t\in\mathbb{R}$，定义

$$g_t(x)=\prod_{\{i,j\}}(x-\beta_{ij}),$$

其中 $\beta_{ij}=\alpha_i+\alpha_j+t\alpha_i\alpha_j$，且 $\{i,j\}$ 遍历 $\{1,\cdots,n\}$ 的一切 2-元子集. 首先，

$$\deg(g_t)=\frac{1}{2}n(n-1)=2^{k-1}m(n-1).$$

现在因为 $k\geqslant1$，所以 $n=2^km$ 是偶数，从而 $n-1$ 是奇数，因此 $m(n-1)$ 是奇数. 于是，如果 $g_t(x)\in\mathbb{R}[x]$，就可以运用归纳假设.

对 $g_t(x)$ 的每个系数 c，存在初等对称函数

$$e(\cdots,y_{ij},\cdots)\in\mathbb{R}[\cdots,y_{ij},\cdots]$$

使得 $c=e(\cdots,\beta_{ij},\cdots)$. 如果定义

$$h(x_1,\cdots,x_n)=e(\cdots,x_i+x_j+tx_ix_j,\cdots),$$

则

$$c=e(\cdots,\alpha_i+\alpha_j+t\alpha_i\alpha_j,\cdots)=h(\alpha_1,\cdots,\alpha_n).$$

每个$\sigma\in S_n$经由$\sigma: x_i+x_j+tx_ix_j \mapsto x_{\sigma i}+x_{\sigma j}+tx_{\sigma i}x_{\sigma j}$作用在$\mathbb{R}[x_1,\cdots,x_n]$上，因此它置换这种形式的多项式的集合．因初等对称函数$e(\cdots,y_{ij},\cdots)$在变量y_{ij}的每个置换下都是不变的，从而$h(x_1,\cdots,x_n)=e(\cdots,x_i+x_j+tx_ix_j,\cdots)$是$x_1,\cdots,x_n$的对称函数．由对称函数的基本定理（习题6.84），存在多项式$\varphi(x)\in\mathbb{R}[x_1,\cdots,x_n]$使得

232

$$h(x_1,\cdots,x_n)=\varphi(e_1(x_1,\cdots,x_n),\cdots,e_n(x_1,\cdots,x_n)).$$

赋值$(x_1,\cdots,x_n)\mapsto(\alpha_1,\cdots,\alpha_n)$给出

$$c=h(\alpha_1,\cdots,\alpha_n)=\varphi(e_1(\alpha_1,\cdots,\alpha_n),\cdots,e_n(\alpha_1,\cdots,\alpha_n)).$$

但$e_r(\alpha_1,\cdots,\alpha_n)$正好是$f(x)$的第$r$个系数，它是实数，从而$c$是实数，即$g_t(x)\in\mathbb{R}[x]$．

由归纳假设，$g_t(x)$对每个$t\in\mathbb{R}$都有复根．有无限个$t\in\mathbb{R}$而只有有限个2-元子集$\{i,j\}$．根据鸽笼原理，存在子集$\{i,j\}$和不同的实数t和s使得$\alpha_i+\alpha_j+t\alpha_i\alpha_j$和$\alpha_i+\alpha_j+s\alpha_i\alpha_j$都是复数［因为$\beta_{ij}$是$g_t(x)$的根］．相减得$(t-s)\alpha_i\alpha_j\in\mathbb{C}$；因$t\neq s$，有$\alpha_i\alpha_j\in\mathbb{C}$，比如$\alpha_i\alpha_j=u$．因$\alpha_i+\alpha_j+t\alpha_i\alpha_j\in\mathbb{C}$，从而$\alpha_i+\alpha_j\in\mathbb{C}$，比如$\alpha_i+\alpha_j=v$．所以$\alpha_i$是$x^2-vx+u$的根，由（ⅱ），二次公式给出所要的$\alpha_i\in\mathbb{C}$．现在对$n\geqslant1$用归纳法可得$f(x)$分裂． ■

下面是第二个证明．

定理（代数基本定理） *每个非常数的多项式$f(x)\in\mathbb{C}[x]$都有复根．*

证明 如同刚才的证明，只需证明每个非常数的$f(x)\in\mathbb{R}[x]$都有复根．设$E/\mathbb{R}$是包含$\mathbb{C}$的$(x^2+1)f(x)$的分裂域．因$\mathbb{R}$有特征0，所以$E/\mathbb{R}$是伽罗瓦扩张，令$G=\mathrm{Gal}(E/\mathbb{R})$是它的伽罗瓦群．现在$|G|=2^mk$，其中$m\geqslant0$且$k$是奇数．由西罗定理（定理5.36），$G$有$2^m$阶子群$H$．设$B=E^H$是相应的中间域，根据伽罗瓦理论的基本定理，次数$[B:\mathbb{R}]$等于指数$[G:H]=k$．但在（ⅴ）中已知$\mathbb{R}$没有大于1的奇数次扩张，因此$k=1$且$G$是2-群．现在$E/\mathbb{C}$也是伽罗瓦扩张，且$\mathrm{Gal}(E/\mathbb{C})\leqslant G$也是2-群．如果这个群不是平凡群，则它有指数为2的子群K．再由基本定理，中间域E^K是$\mathbb{C}$的次数为2的扩张，此与（ⅲ）矛盾．由此可知$[E:\mathbb{C}]=1$，即$E=\mathbb{C}$．但E是$f(x)$在$\mathbb{C}$上的分裂域，所以$f(x)$有复根． ■

现在证明伽罗瓦定理的逆定理（仅在特征0时成立）：伽罗瓦群的可解性蕴涵多项式运用根式可解．为此，有必要证明某种域扩张是纯扩张，并且将用到范数（在代数数论中十分自然地产生范数，例如，定理3.66即费马二平方和定理的证明中就用到它）．

定义 *如果E/k是伽罗瓦扩张，且$u\in E^\times$，定义u的***范数***$N(u)$为*

$$N(u)=\prod_{\sigma\in\mathrm{Gal}(E/k)}\sigma(u).$$

下面是范数的一些初等性质，它们的简单证明留作习题．

233

（ⅰ）如果$u\in E^\times$，则$N(u)\in k^\times$（因为$N(u)\in E^G=k$）．

（ⅱ）$N(uv)=N(u)N(v)$，从而$N: E^\times\to k^\times$是同态．

（ⅲ）如果$a\in k$，则$N(a)=a^n$，其中$n=[E:k]$．

（ⅳ）如果$\sigma\in G$且$u\in E^\times$，则$N(\sigma(u))=N(u)$．

给定一个同态，我们关注它的核和象．范数的象不容易计算，下面的结果（它是1897年希尔伯特提出的关于代数数论的第九十个定理）在一种特殊情形中计算了范数的核．

定理4.50（希尔伯特定理90） *设E/k是伽罗瓦扩张，它的伽罗瓦群$G=\mathrm{Gal}(E/k)$是n阶循环群，比如生成元为σ．如果$u\in E^\times$，则$N(u)=1$当且仅当存在$v\in E^\times$使得$u=v\sigma(v)^{-1}$．*

证明 如果 $u = v\sigma(v)^{-1}$，则

$$\begin{aligned}N(u) &= N(v\sigma(v)^{-1})\\ &= N(v)N(\sigma(v)^{-1})\\ &= N(v)N(\sigma(v))^{-1}\\ &= N(v)N(v)^{-1} = 1.\end{aligned}$$

反之，设 $N(u) = 1$. 在 $E^\times$ 中定义"偏范数"：

$$\begin{aligned}\delta_0 &= u,\\ \delta_1 &= u\sigma(u),\\ \delta_2 &= u\sigma(u)\sigma^2(u),\\ &\vdots\\ \delta_{n-1} &= u\sigma(u)\cdots\sigma^{n-1}(u).\end{aligned}$$

注意 $\delta_{n-1} = N(u) = 1$. 易知

$$\text{对一切 } 0 \leqslant i \leqslant n-2,\ u\sigma(\delta_i) = \delta_{i+1}. \tag{4}$$

由特征标 $1, \sigma, \sigma^2, \cdots, \sigma^{n-1}$ 的无关性，存在 $y \in E$ 使得

$$\delta_0 y + \delta_1\sigma(y) + \cdots + \delta_{n-2}\sigma^{n-2}(y) + \sigma^{n-1}(y) \neq 0;$$

把这个和叫做 z. 用等式 (4)，容易验证

$$\begin{aligned}\sigma(z) &= \sigma(\delta_0)\sigma(y) + \sigma(\delta_1)\sigma^2(y) + \cdots + \sigma(\delta_{n-2})\sigma^{n-1}(y) + \sigma^n(y)\\ &= u^{-1}\delta_1\sigma(y) + u^{-1}\delta_2\sigma^2(y) + \cdots + u^{-1}\delta_{n-1}\sigma^{n-1}(y) + y\\ &= u^{-1}(\delta_1\sigma(y) + \delta_2\sigma^2(y) + \cdots + \delta_{n-1}\sigma^{n-1}(y)) + u^{-1}\delta_0 y\\ &= u^{-1}z.\end{aligned}$$

■ [234]

系 4.51 *设 E/k 是素数 p 次伽罗瓦扩张. 如果 k 包含一个 p 次单位原根 ω，则 $E = k(z)$，其中 $z^p \in k$，从而 E/k 是 p 型纯扩张.*

证明 伽罗瓦群 $G = \mathrm{Gal}(E/k)$ 的阶为 p，因此是循环群，令 σ 为生成元. 因为 $\omega \in k$，从而 $N(\omega) = \omega^p = 1$. 根据希尔伯特定理 90，对某个 $z \in E$ 有 $\omega = z\sigma(z)^{-1}$，因此 $\sigma(z) = \omega^{-1}z$，于是 $\sigma(z^p) = (\omega^{-1}z)^p = z^p$. 因为 σ 生成 G，所以 $z^p \in E^G$，然而因为 E/k 是伽罗瓦扩张，所以有 $E^G = k$，从而 $z^p \in k$. 注意 $z \notin k$，否则 $\omega = 1$，从而 $k(z) \neq k$ 是一个中间域. 因为 $[E:k] = p$ 是素数，所以 $E = k(z)$，因此 E 没有真中间域. ■

我们承认介绍希尔伯特定理 90 不仅因为用它的推论可以证明伽罗瓦定理，而且因为它是一个著名的结果，是同调代数的早期实例（见系 10.129）. 下面是 E. Houston 对系 4.51 的一个优美证明（我们提醒读者，这个证明使用了我们尚未引入的特征值的课题）.

命题 4.52 *设 E/k 是素数 p 次伽罗瓦扩张. 如果 k 包含一个 p 次单位原根 ω，则 $E = k(z)$，其中 $z^p \in k$，从而 E/k 是 p 型纯扩张.*

证明 因 E/k 是 p 次伽罗瓦扩张，它的伽罗瓦群 $G = \mathrm{Gal}(E/k)$ 的阶为 p，所以是循环群：$G = \langle\sigma\rangle$. 把 E 看作 k 上的向量空间. 如果 $a \in k$ 且 $u \in E$，则因 $\sigma \in \mathrm{Gal}(E/k)$（从而 σ 固定 k），有 $\sigma(au) = \sigma(a)\sigma(u) = a\sigma(u)$，由此可以把 $\sigma: E \to E$ 看作一个线性变换. 现在根据拉格朗日定理，因 $\sigma^p = 1_E$，所以 σ 满足多项式 $x^p - 1$. 而 σ 不能满足较小次数的多项式，否则与特征标 $1, \sigma, \sigma^2, \cdots, \sigma^{p-1}$ 无关矛盾，所以 $x^p - 1$ 是 σ 的极小多项式，从而每个 p 次单位根都是 σ 的特征值. 根据假设，$\omega^{-1} \in k$，所以存在 σ 的特征向量 $z \in E$ 使得 $\sigma(z) = \omega^{-1}z$（注意 $z \notin k$，因为它不被 σ 固定）. 因此

$\sigma(z^p)=(\sigma(z))^p=(\omega^{-1})^p z^p=z^p$，由此，$z^p\in E^G=k$. 现在 $p=[E:k]=[E:k(z)][k(z):k]$，因 p 是素数且 $[k(z):k]\neq 1$，所以有 $[E:k(z)]=1$；即 $E=k(z)$，从而 E/k 是纯扩张. ■

定理 4.53（伽罗瓦） 设 k 是特征 0 的域，E/k 是伽罗瓦扩张，并设 $G=\mathrm{Gal}(E/k)$ 是可解群，则 E 可以嵌入 k 的一个根式扩张.

所以，特征 0 的域上的一个多项式的伽罗瓦群是可解群当且仅当该多项式是运用根式可解的.

注 特征 p 中的一个反例在命题 4.56 中给出.

证明 因 G 可解，它有素数指数的正规子群 H，比如指数为 p. 令 ω 是 p 次单位原根，因为 k 有特征 0，ω 必在某个扩域中. 分两种情形.

235

情形（ⅰ）：$\omega\in k$.

对 $[E:k]$ 用归纳法证明该陈述. 基础步显然为真，因为 $k=E$ 是它自己的根式扩张. 关于归纳步，考虑中间域 E^H. 现在由系 4.36，E/E^H 是伽罗瓦扩张，且 $\mathrm{Gal}(E/E^H)$ 是可解的，它是可解群 G 的子群. 因 $[E:E^H]<[E:k]$，归纳假设给出根式扩张塔 $E^H\subseteq R_1\subseteq\cdots\subseteq R_t$，其中 $E\subseteq R_t$. 因为 $H\lhd G$，所以 E^H/k 是伽罗瓦扩张，由基本定理，它的指数 $[G:H]=p=[E^H:k]$. 运用系 4.51（或命题 4.52）得 $E^H=k(z)$，其中 $z^p\in k$，即 E^H/k 是纯扩张. 因此上面的根式扩张塔可以加进一个前缀 $k\subseteq E^H$ 来加长，从而表明 R_t/k 是根式扩张.

情形（ⅱ）：一般情形.

设 $k^*=k(\omega)$，且定义 $E^*=E(\omega)$. 我们断言 E^*/k 是伽罗瓦扩张. 因 E/k 是伽罗瓦扩张，所以它是某个可分多项式 $f(x)\in k[x]$ 的分裂域，从而 E^* 是 $f(x)(x^p-1)$ 在 k 上的分裂域. 但因 k 有特征 0，所以 x^p-1 是可分的，从而 E^*/k 是伽罗瓦扩张. 所以由系 4.36，E^*/k^* 也是伽罗瓦扩张. 令 $G^*=\mathrm{Gal}(E^*/k^*)$，根据习题 4.5 的配连无理性，存在单射 $\psi:G^*\to G=\mathrm{Gal}(E/k)$，从而 G^* 是可解的，它同构于可解群的一个子群. 因 $\omega\in k^*$，第一种情形证明存在根式扩张塔 $k^*\subseteq R_1^*\subseteq\cdots\subseteq R_m^*$ 使得 $E\subseteq E^*\subseteq R_m^*$. 而 $k^*=k(\omega)$ 是纯扩张，从而前面的根式扩张塔可以加进前缀 $k\subseteq k^*$ 来加长，由此表明 R_m^*/k 是根式扩张. ■

我们现在有经典公式存在性的另一个证明.

系 4.54 如果 k 有特征 0，则每个次数 $\deg(f)\leqslant 4$ 的 $f(x)\in k[x]$ 都是运用根式可解的.

证明 设 G 是 $f(x)$ 的伽罗瓦群，则 G 同构于 S_4 的子群. 但 S_4 是可解群，从而 S_4 的每个子群也是可解群. 由伽罗瓦定理，$f(x)$ 运用根式可解. ■

假设已知多项式 $f(x)\in\mathbb{Q}[x]$ 的伽罗瓦群 G 且 G 可解. 我们能够运用这一信息求出 $f(x)$ 的根吗？答案是肯定的. 要知道究竟怎样做，建议读者参考 Gaal 所著的《Classical Galois Theory with Examples》.

1827 年，阿贝尔证明：如果多项式 $f(x)$ 的伽罗瓦群是可交换的，则 $f(x)$ 运用根式可解（当然，伽罗瓦群还没有定义），这个结果立即被 1830 年证明的伽罗瓦定理所取代，但这是阿贝尔群名称的由来.

W. Feit 和 J. G. Thompson (1963) 的一个更深入的定理说：每个奇数阶群都是可解的. 由此，如果 k 是特征 0 的域，且多项式 $f(x)\in k[x]$ 的伽罗瓦群的阶为奇数，或等价地说，它在 k 上的分裂域是奇数次的，则 $f(x)$ 运用根式可解.

236

下一命题给出一个例子说明伽罗瓦定理的逆定理在特征为素数时不成立.

引理 4.55 如果 $k=\mathbb{F}_p(t)$，它是 $\mathbb{F}_p$ 上的有理函数域，则 $f(x)=x^p-x-t$ 在 k 中无根.

证明 如果在 k 中有 $f(x)$ 的根 α，则存在 $g(t),h(t)\in \mathbb{F}_p[t]$ 使得 $\alpha=g(t)/h(t)$. 可以假定 $(g,h)=1$. 因 α 是 $f(x)$ 的根，所以有 $(g/h)^p-(g/h)=t$. 通分得 $\mathbb{F}_p[t]$ 中的等式 $g^p-h^{p-1}g=th^p$，因此 $g\mid th^p$. 因 $(g,h)=1$，有 $g\mid t$，从而 $g(t)=at$ 或 $g(t)$ 是常数，比如 $g(t)=b$，其中 $a,b\in\mathbb{F}_p$. 在上面的等式中把 $h^{p-1}g$ 移到右端表明 $h\mid g^p$，而 $(g,h)=1$ 迫使 h 是常数. 由此可知，如果 $\alpha=g/h$，则 $\alpha=at$ 或 $\alpha=b$. 在第一种情形中，

$$
\begin{aligned}
0&=\alpha^p-\alpha-t\\
&=(at)^p-(at)-t\\
&=a^pt^p-at-t\\
&=at^p-at-t \qquad \text{根据}\mathbb{F}_p\text{中的费马定理}\\
&=t(at^{p-1}-a-1).
\end{aligned}
$$

由此 $at^{p-1}-a-1=0$. 而 $a\neq0$，这与 t 是 $\mathbb{F}_p$ 上的超越元素矛盾. 在第二种情形中，$\alpha=b\in\mathbb{F}_p$. 根据费马定理，因 $f(b)=b^p-b-t=-t$，所以 b 不是 $f(x)$ 的根. 由此 $f(x)$ 在 k 中不可能有根 α. ■

命题 4.56 *设 p 是素数，并设 $k=\mathbb{F}_p(t)$，则 $f(x)=x^p-x-t$ 在 k 上的伽罗瓦群是 p 阶循环群，而 $f(x)$ 在 k 上不是运用根式可解的.*

证明 设 α 是 $f(x)$ 的根，易知 $f(x)$ 的根是 $\alpha+i$，其中 $0\leqslant i<p$，这是因为费马定理在 $\mathbb{F}_p$ 中给出 $i^p=i$，从而

$$(\alpha+i)^p-(\alpha+i)-t=\alpha^p+i^p-\alpha-i-t=\alpha^p-\alpha-t=0.$$

由此 $f(x)$ 是可分多项式且 $k(\alpha)$ 是 $f(x)$ 在 k 上的分裂域. 我们断言 $f(x)$ 在 $k[x]$ 中不可约. 假设 $f(x)=g(x)h(x)$，其中

$$g(x)=x^d+c_{d-1}x^{d-1}+\cdots+c_0\in k[x]$$

且 $0<d<\deg(f)=p$，则 $g(x)$ 是形如 $x-(\alpha+i)$ 的 d 个因式的积. 现在 $-c_{d-1}\in k$ 是根的和：$-c_{d-1}=d\alpha+j$，其中 $j\in\mathbb{F}_p$，因此 $d\alpha\in k$. 然而因 $0<d<p$，在 k 中 $d\neq0$，由此迫使 $\alpha\in k$，这与引理矛盾. 所以 $f(x)$ 是 $k[x]$ 中的不可约多项式. 因 $\deg(f)=p$，有 $[k(\alpha):k]=p$，又因为 $f(x)$ 是可分的，有 $|\mathrm{Gal}(k(\alpha)/k)|=[k(\alpha):k]=p$. 所以 $\mathrm{Gal}(k(\alpha)/k)\cong\mathbb{I}_p$.

考虑某种合适的单位根会带来方便. 令 Ω 是一切 q 次单位根的集合，其中 $q<p$ 是 $p!$ 的一个素因数. 我们断言 $\alpha\notin k(\Omega)$. 一方面，如果 $n=\prod_{q<p}q$，则 Ω 包含在 x^n-1 的分裂域中，从而根据定理 4.3，$[k(\Omega):k]\mid n!$. 由此 $p\nmid[k(\Omega):k]$. 另一方面，如果 $\alpha\in k(\Omega)$，则 $k(\alpha)\subseteq k(\Omega)$ 且 $[k(\Omega):k]=[k(\Omega):k(\alpha)][k(\alpha):k]=p[k(\Omega):k(\alpha)]$. 因此 $p\mid[k(\Omega):k]$，从而产生矛盾. 237

如果 $f(x)$ 在 $k(\Omega)$ 上运用根式可解，则有根式扩张

$$k(\Omega)=B_0\subseteq B_1\subseteq\cdots\subseteq B_r$$

使得 $k(\Omega,\alpha)\subseteq B_r$. 可以假定对每个 $i\geqslant1$，B_i/B_{i-1} 是素数型的，即 $B_i=B_{i-1}(u_i)$，其中 $u_i^{q_i}\in B_{i-1}$ 且 q_i 是素数. 存在某个 $j\geqslant1$ 使得 $\alpha\in B_j$ 但 $\alpha\notin B_{j-1}$. 为简化记号，我们设 $u_j=u,q_j=q$，$B_{j-1}=B$ 和 $B_j=B'$，于是 $B'=B(u)$，$u^q=b\in B$，$\alpha\in B'$ 和 $\alpha,u\notin B$. 我们断言在 $k[x]$ 中不可约多项式 $f(x)=x^p-x-t$ 在 $B[x]$ 中也不可约. 由习题 4.5 的配连无理性，限制函数给出单射 $\mathrm{Gal}(B(\alpha)/B)\to\mathrm{Gal}(k(\alpha)/k)\cong\mathbb{I}_p$. 如果 $\mathrm{Gal}(B(\alpha)/B)=\{1\}$，则 $B(\alpha)=B$ 且 $\alpha\in B$，这是一个矛盾. 所以 $\mathrm{Gal}(B(\alpha)/B)\cong\mathbb{I}_p$，由习题 4.11，$f(x)$ 在 $B[x]$ 中不可约.

因 $u\notin B'$ 且 B 包含一切 q 次单位根，命题 3.126 表明 x^q-b 在 $B[x]$ 中不可约，这是因为 x^q-b

在 $B[x]$ 中不分裂. 现在 $B'=B(u)$ 是 x^q-b 的分裂域，从而 $[B':B]=q$. 我们有 $B\subsetneq B(\alpha)\subseteq B'$，且

$$q=[B':B]=[B':B(\alpha)][B(\alpha):B].$$

因 q 是素数，$[B':B(\alpha)]=1$，即 $B'=B(\alpha)$，从而 $q=[B':B]$. 因 α 是不可约多项式 $f(x)=x^p-x-t\in B[x]$ 的根，有 $[B(\alpha):B]=p$，所以 $q=p$. 现在因为 α 是一个可分元素，根据命题 4.38，$B(u)=B'=B(\alpha)$ 是可分扩张. 从而 $u\in B'$ 也是可分元素，这与 $\mathrm{irr}(u,B)=x^q-b=x^p-b=(x-u)^p$ 有重根矛盾.

我们已经证明了 $f(x)$ 在 $k(\Omega)$ 上运用根式不可解，由此 $f(x)$ 在 k 上运用根式不可解，这是因为有根式扩张 $k=R_0\subseteq R_1\subseteq\cdots\subseteq R_t$ 使得 $k(\alpha)\subseteq R_t$，由此 $k(\Omega)=R_0(\Omega)\subseteq R_1(\Omega)\subseteq\cdots\subseteq R_t(\Omega)$ 表明 $f(x)$ 在 $k(\Omega)$ 上运用根式可解，从而产生矛盾. ■

在计算伽罗瓦群中，多项式的判别式是有用的.

定义 如果 $f(x)=\prod_i(x-\alpha_i)\in k[x]$，其中 k 是域，定义

$$\Delta=\prod_{i<j}(\alpha_i-\alpha_j),$$

并定义**判别式**为 $D=D(f)=\Delta^2=\prod_{i<j}(\alpha_i-\alpha_j)^2$.

显然，$f(x)$ 有重根当且仅当它的判别式 $D=0$.

乘积 $\Delta=\prod_{i<j}(\alpha_i-\alpha_j)$ 对每个不同的指标对 (i,j) 有一个因子 $\alpha_i-\alpha_j$（限制 $i<j$ 防止一个指标对出现两次）. 如果 E/k 是 $f(x)$ 的分裂域且 $G=\mathrm{Gal}(E/k)$，则每个 $\sigma\in G$ 置换根，从而 σ 置换一切不同的对. 然而，可能发生这样的情况：$i<j$ 而 $\sigma(\alpha_i)-\sigma(\alpha_j)$ 中的下标处于反序. 例如，假设一个三次多项式的根为 $\alpha_1,\alpha_2,\alpha_3$，并假设存在 $\sigma\in G$ 使得 $\sigma(\alpha_1)=\alpha_2,\sigma(\alpha_2)=\alpha_1,\sigma(\alpha_3)=\alpha_3$，则

$$\begin{aligned}\sigma(\Delta)&=(\sigma(\alpha_1)-\sigma(\alpha_2))(\sigma(\alpha_1)-\sigma(\alpha_3))(\sigma(\alpha_2)-\sigma(\alpha_3))\\&=(\alpha_2-\alpha_1)(\alpha_2-\alpha_3)(\alpha_1-\alpha_3)\\&=-(\alpha_1-\alpha_2)(\alpha_2-\alpha_3)(\alpha_1-\alpha_3)\\&=-\Delta.\end{aligned}$$

一般来说，出现在 $\sigma(\Delta)$ 中的每一项 $\alpha_i-\alpha_j$ 都有可能变号. 由此可知，对一切 $\sigma\in\mathrm{Gal}(E/k)$，$\sigma(\Delta)=\pm\Delta$. 自然会认为 Δ^2 比 Δ 好，因为 Δ 不仅依赖于 $f(x)$ 的根，还依赖于根的排列次序，而 $D=\Delta^2$ 不依赖于根的排列次序. 关于判别式和交错群 A_n 之间的联系，见命题4.59(ⅱ).

命题 4.57 如果 $f(x)\in k[x]$ 是可分多项式，则它的判别式 D 在 k 中.

证明 设 E/k 是 $f(x)$ 的分裂域，因 $f(x)$ 可分，根据定理 4.34，E/k 是伽罗瓦扩张. 每个 $\sigma\in\mathrm{Gal}(E/k)$ 置换 $f(x)$ 的根 $u_1,\cdots,u_n$，且已知 $\sigma(\Delta)=\pm\Delta$. 所以

$$\sigma(D)=\sigma(\Delta^2)=\sigma(\Delta)^2=(\pm\Delta)^2=D,$$

从而 $D\in E^G$. 因 E/k 是伽罗瓦扩张，所以有 $E^G=k$，因此 $D\in k$. ■

如果 $f(x)=x^2+bx+c$，则二次公式给出 $f(x)$ 的根：

$$\alpha=\frac{1}{2}(-b+\sqrt{b^2-4c})\text{和}\beta=\frac{1}{2}(-b-\sqrt{b^2-4c}).$$

从而

$$D=\Delta^2=(\alpha-\beta)^2=b^2-4c.$$

如果 $f(x)$ 是三次多项式有根 α,β,γ，则

238

$$D = \Delta^2 = (\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2;$$

如何由 $f(x)$ 的系数来计算判别式 D 是不明显的.

定义 多项式 $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 \in k[x]$ 称为**约化**的，如果 $c_{n-1}=0$. 如果 $f(x)$ 是 n 次首一多项式且在 k 中 $c_{n-1}\neq 0$，其中 $\mathrm{char}(k) = 0$，则它的**相伴约化多项式**是

$$\tilde{f}(x) = f\left(x - \frac{1}{n}c_{n-1}\right).$$

如果 $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 \in k[x]$ 且 $\beta \in k$ 是 $\tilde{f}(x)$ 的根，则

$$0 = \tilde{f}(\beta) = f\left(\beta - \frac{1}{n}c_{n-1}\right).$$

因此 β 是 $\tilde{f}(x)$ 的根当且仅当 $\beta - \frac{1}{n}c_{n-1}$ 是 $f(x)$ 的根.

239

定理 4.58 设 k 是特征 0 的域.

（i）多项式 $f(x) \in k[x]$ 和它的相伴约化多项式 $\tilde{f}(x)$ 有相同的判别式.

（ii）约化三次多项式 $\tilde{f}(x) = x^3 + qx + r$ 的判别式是

$$D = -4q^3 - 27r^2.$$

证明 （i）如果 $f(x) = \sum c_i x^i$ 的根是 $\alpha_1, \cdots, \alpha_n$，则 $\tilde{f}(x)$ 的根是 $\beta_1, \cdots, \beta_n$，其中 $\beta_i = \alpha_i + \frac{1}{n}c_{n-1}$. 所以对一切 i, j, $\beta_i - \beta_j = \alpha_i - \alpha_j$,

$$\prod_{i<j}(\alpha_i - \alpha_j) = \prod_{i<j}(\beta_i - \beta_j),$$

判别式是它们的平方，所以相等.

（ii）三次公式给出 $\tilde{f}(x)$ 的根是

$$\alpha = g + h, \beta = \omega g + \omega^2 h, \gamma = \omega^2 g + \omega h,$$

其中 $g = \left[\frac{1}{2}(-r + \sqrt{R})\right]^{1/3}$, $h = -q/3g$, $R = r^2 + \frac{4}{27}q^3$，且 ω 是三次单位根. 因为 $\omega^3 = 1$，有

$$\begin{aligned}\alpha - \beta &= (g+h) - (\omega g + \omega^2 h)\\ &= (g - \omega^2 h) - (\omega g - h)\\ &= (g - \omega^2 h) - (g - \omega^2 h)\omega\\ &= (g - \omega^2 h)(1-\omega).\end{aligned}$$

类似的计算给出

$$\alpha - \gamma = (g+h) - (\omega^2 g + \omega h) = (g - \omega h)(1 - \omega^2)$$

和

$$\beta - \gamma = (\omega g + \omega^2 h) - (\omega^2 g + \omega h) = (g - h)\omega(1-\omega).$$

由此

$$\Delta = (g-h)(g-\omega h)(g-\omega^2 h)\omega(1-\omega^2)(1-\omega)^2.$$

根据习题 4.14，有 $\omega(1-\omega^2)(1-\omega)^2 = 3\mathrm{i}\sqrt{3}$；此外恒等式

$$x^3 - 1 = (x-1)(x-\omega)(x-\omega^2)$$

以及 $x = g/h$ 给出

$$(g-h)(g-\omega h)(g-\omega^2 h) = g^3 - h^3 = \sqrt{R}$$

（208 页上已知 $g^3 - h^3 = \sqrt{R}$）. 所以 $\Delta = 3\mathrm{i}\sqrt{3}\sqrt{R}$，从而

240

$$D = \Delta^2 = -27R = -27r^2 - 4q^3.$$ ■

注 设 k 是域，且设 $f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ 和 $g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 \in k[x]$，定义它们的**结式**为

$$\mathrm{Res}(f,g) = \det(M),$$

其中 $M = M(f,g)$ 是 $(m+n)\times(m+n)$ 矩阵.

$$M = \begin{bmatrix} a_m & a_{m-1} & \cdots & a_1 & a_0 & & \\ & a_m & a_{m-1} & \cdots & a_1 & a_0 & \\ & & a_m & a_{m-1} & \cdots & a_1 & a_0 \\ & & & \cdots & & & \\ b_n & b_{n-1} & \cdots & b_1 & b_0 & & \\ & b_n & b_{n-1} & \cdots & b_1 & b_0 & \\ & & b_n & b_{n-1} & \cdots & b_1 & b_0 \\ & & & \cdots & & & \end{bmatrix};$$

有 n 行是 $f(x)$ 的系数 a_i，m 行是 $g(x)$ 的系数 b_j，除了所显示的这些元素外，其他元素均为 0. 可以证明 $\mathrm{Res}(f,g)=0$ 当且仅当 f 和 g 有非常数的公因式. 我们在这里提起结式是因为可以用它来计算判别式：

$$D(f) = (-1)^{n(n-1)/2}\mathrm{Res}(f,f'),$$

其中 $f'(x)$ 是 $f(x)$ 的导数. 见 Dummit 和 Foote 所著的《Abstract Algebra》600～602 页中的习题.

下面是用判别式计算伽罗瓦群的一种方法.

命题 4.59 设 k 是特征 $\neq 2$ 的域，$f(x)\in k[x]$ 是无重根的 n 次多项式，且 $D=\Delta^2$ 是它的判别式. 设 E/k 是 $f(x)$ 的分裂域，并把 $G=\mathrm{Gal}(E/k)$ 看作 S_n 的子群（如同定理 4.3 中一样）.

（ⅰ）如果 $H = A_n\cap G$，则 $E^H = k(\Delta)$.

（ⅱ）G 是 A_n 的子群当且仅当 $\sqrt{D}\in k$.

证明 （ⅰ）第二同构定理给出 $H=(G\cap A_n)\lhd G$ 且

$$[G:H] = [G:A_n\cap G] = [A_nG:A_n] \leqslant [S_n:A_n] = 2.$$

由伽罗瓦理论的基本定理（因为 $f(x)$ 无重根，因而它是可分的，所以可以应用该定理），$[E^H:k]=[G:H]$，从而 $[E^H:k]=[G:H]\leqslant 2$. 由习题 4.25，我们有 $k(\Delta)\subseteq E^{A_n}$，从而 $k(\Delta)\subseteq E^H$. 所以，

241

$$[E^H:k] = [E^H:k(\Delta)][k(\Delta):k] \leqslant 2. \qquad (5)$$

有两种情形. 如果 $[E^H:k]=1$，则 (5) 式中的每个因子都是 1，特别是 $[E^H:k(\Delta)]=1$，从而 $E^H=k(\Delta)$. 如果 $[E^H:k]=2$，则 $[G:H]=2$ 且存在 $\sigma\in G$，$\sigma\notin A_n$，从而 $\sigma(\Delta)=-\Delta$. 现在因 $f(x)$ 无重根，所以 $\Delta\neq 0$，又因为 k 的特征不是 2，所以 $-\Delta\neq\Delta$. 因此 $\Delta\notin E^G=k$ 且 $[k(\Delta):k]>1$. 由此，从 (5) 式得 $[E^H:k(\Delta)]=1$ 且 $E^H=k(\Delta)$.

（ⅱ）下面三个关系式等价：$G\leqslant A_n$；$H=G\cap A_n=G$；$E^H=E^G=k$. 因根据（ⅰ），$E^H=k(\Delta)$，所以 $E^H=k$ 等价于 $k(\Delta)=k$；即 $\Delta=\sqrt{D}\in k$. ■

我们现在说明如何计算 $\mathbb{Q}$ 上低次数多项式的伽罗瓦群.

如果 $f(x)\in\mathbb{Q}[x]$ 是二次多项式，则它的伽罗瓦群的阶为 1 或 2（因为对称群 S_2 的阶为 2）. 如果 $f(x)$ 分裂，伽罗瓦群的阶为 1；如果 $f(x)$ 不分裂，即 $f(x)$ 不可约，则阶为 2.

如果 $f(x)\in\mathbb{Q}[x]$ 是有有理根的三次多项式，则它的伽罗瓦群和它的二次因式的伽罗瓦群相同. 否则，$f(x)$ 不可约，由系 4.9，因 $|G|$ 是 3 的倍数且 $G\leqslant S_3$，从而 $G\cong A_3\cong \mathbb{I}_3$ 或 $G\cong S_3$.

命题 4.60 设 $f(x)\in\mathbb{Q}[x]$ 是三次不可约多项式，伽罗瓦群为 G，判别式为 D.

（ⅰ）$f(x)$ 恰有一个实根当且仅当 $D<0$. 此时 $G\cong S_3$.

（ⅱ）$f(x)$ 有三个实根当且仅当 $D>0$. 此时或者 $\sqrt{D}\in\mathbb{Q}$ 且 $G\cong\mathbb{I}_3$，或者 $\sqrt{D}\notin\mathbb{Q}$ 且 $G\cong S_3$.

证明 首先注意 $D\neq 0$：因为$\mathbb{Q}$有特征 0，$\mathbb{Q}$ 上的不可约多项式没有重根. 如果 $f(x)$ 有三个实根，则 Δ 是实数，且 $D=\Delta^2>0$. 另一种可能是 $f(x)$ 有一个实根 α 和两个复根：$\beta=u+\mathrm{i}v$ 和 $\overline{\beta}=u-\mathrm{i}v$. 因 $\beta-\overline{\beta}=2\mathrm{i}v$ 和 $\alpha=\overline{\alpha}$，有

$$\begin{aligned}\Delta &= (\alpha-\beta)(\alpha-\overline{\beta})(\beta-\overline{\beta})\\ &= (\alpha-\beta)(\overline{\alpha-\beta})(\beta-\overline{\beta})\\ &= |\alpha-\beta|^2(2\mathrm{i}v),\end{aligned}$$

从而 $D=\Delta^2=-4v^2|\alpha-\beta|^4<0$.

设 $E/\mathbb{Q}$ 是 $f(x)$ 的分裂域. 如果 $f(x)$ 恰有一个实根 α，则 $E\neq\mathbb{Q}(\alpha)$，因此 $|G|>3$ 且 $G\cong S_3$. 如果 $f(x)$ 有三个实根，则 $D>0$ 且 $\sqrt{D}$是实数. 由命题4.59(ⅱ)，$G\cong A_3\cong\mathbb{I}_3$ 当且仅当$\sqrt{D}$是有理数，因此如果$\sqrt{D}$是无理数，$G\cong S_3$. ■

例 4.61 由定理 3.43，多项式 $f(x)=x^3-2\in\mathbb{Q}[x]$ 是不可约的. 它的判别式是 $D=-108$，因此它有一个实根. 因 $\sqrt{-108}\notin\mathbb{Q}$（它甚至不是实数），所以 $f(x)$ 的伽罗瓦群不包含在 A_3 中，因此它的伽罗瓦群为 S_3.

由定理 3.43 或艾森斯坦准则，多项式 $f(x)=x^3-4x+2\in\mathbb{Q}[x]$ 是不可约的，它的判别式是 $D=148$，从而它有三个实根. 因为 $\sqrt{148}$是无理数，所以伽罗瓦群是 S_3.

由定理 3.43，多项式 $f(x)=x^3-48x+64\in\mathbb{Q}[x]$ 是不可约的，判别式是 $D=2^{12}3^4$，从而 $f(x)$ 有三个实根. 因为$\sqrt{D}$是有理数，所以伽罗瓦群是 $A_3\cong\mathbb{I}_3$. ■

242

在考察四次多项式之前，我们注意到如果 d 是 $|S_4|=24$ 的因数，则 S_4 有 d 阶子群（习题 5.23）. 如果 $d=4$，则 $\mathbf{V}$ 和$\mathbb{I}_4$ 是不同构的 d 阶子群，对任一其他的因数 d，任两个 d 阶子群同构. 由此可知一个四次多项式的伽罗瓦群的同构由它的阶所确定，除非 $|G|=4$.

考虑（约化）四次多项式 $f(x)=x^4+qx^2+rx+s\in\mathbb{Q}[x]$. 设 $E/\mathbb{Q}$ 是它的分裂域，并设 $G=\mathrm{Gal}(E/\mathbb{Q})$ 是它的伽罗瓦群. [由习题 4.15，不失一般性，假设 $f(x)$ 是约化的.] 如果 $f(x)$ 有有理根 α，则 $f(x)=(x-\alpha)c(x)$，它的伽罗瓦群和三次因式 $c(x)$ 的相同，而三次多项式的伽罗瓦群已经讨论过了. 假设 $f(x)=h(x)\ell(x)$ 是两个不可约二次多项式的积，令 α 是 $h(x)$ 的根和 β 是 $\ell(x)$ 的根. 如果 $\mathbb{Q}(\alpha)\cap\mathbb{Q}(\beta)=\mathbb{Q}$，则习题4.17(ⅳ)证明 $G\cong\mathbf{V}$，即四群；否则 $\alpha\in\mathbb{Q}(\beta)$，从而 $\mathbb{Q}(\beta)=\mathbb{Q}(\alpha,\beta)=E$，且 G 的阶为 2.

剩下的情形是 $f(x)$ 不可约. 现在基本的想法是比较 G 和四群 $\mathbf{V}$，也就是 S_4 的正规子群

$$\mathbf{V}=\{(1),(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\},$$

从而可以识别 $\mathbf{V}\cap G$ 的固定域. 如果 $f(x)$ 的四个（必须不同）根是 $\alpha_1,\alpha_2,\alpha_3,\alpha_4$，考虑数 [根据命题 4.63(ⅱ)，它们是不同的]：

$$\begin{cases}u=(\alpha_1+\alpha_2)(\alpha_3+\alpha_4),\\ v=(\alpha_1+\alpha_3)(\alpha_2+\alpha_4),\\ w=(\alpha_1+\alpha_4)(\alpha_2+\alpha_3).\end{cases}\tag{6}$$

显然，如果$\sigma \in \mathbf{V} \cap G$,则$\sigma$固定$u,v$和$w$. 反之，如果$\sigma \in S_4$固定$u=(\alpha_1+\alpha_2)(\alpha_3+\alpha_4)$，则

$$\sigma \in \mathbf{V} \cup \{(1\ 2),(3\ 4),(1\ 3\ 2\ 4),(1\ 4\ 2\ 3)\}.$$

然而，后面的四个置换没有一个能够同时固定v和w，从而$\sigma \in G$固定每个u,v,w当且仅当$\sigma \in \mathbf{V} \cap G$. 所以

$$E^{\mathbf{V} \cap G} = \mathbb{Q}(u,v,w).$$

定义 $f(x)=x^4+qx^2+rx+s$的**预解三次多项式**是指

$$g(x)=(x-u)(x-v)(x-w),$$

[243] 其中u,v,w是(6)式中定义的数.

命题 4.62 $f(x)=x^4+qx^2+rx+s$的预解三次多项式是

$$g(x)=x^3-2qx^2+(q^2-4s)x+r^2.$$

证明 如果$f(x)=(x^2+jx+\ell)(x^2-jx+m)$，则在209页对四次公式的讨论中我们知道$j^2$是

$$h(x)=x^3+2qx^2+(q^2-4s)x-r^2$$

的根. 它和命题声称的$g(x)$的表达式只相差二次项和常数项的符号. 于是，数β是$h(x)$的根当且仅当$-\beta$是$g(x)$的根.

标记$f(x)$的四个根$\alpha_1,\alpha_2,\alpha_3,\alpha_4$使得$\alpha_1,\alpha_2$是$x^2+jx+\ell$的根,$\alpha_3,\alpha_4$是$x^2-jx+m$的根. 则$j=-(\alpha_1+\alpha_2)$，$-j=-(\alpha_3+\alpha_4)$，所以，

$$u=(\alpha_1+\alpha_2)(\alpha_3+\alpha_4)=-j^2,$$

因$h(j^2)=0$，所以$-u$是$h(x)$的根.

现在把$f(x)$分解为两个二次多项式，比如

$$f(x)=(x^2+\tilde{j}x+\tilde{\ell})(x^2-\tilde{j}x+\tilde{m}),$$

其中α_1,α_3是第一个因式的根，α_2,α_4是第二个因式的根. 用与前面同样的论证可证明

$$v=(\alpha_1+\alpha_3)(\alpha_2+\alpha_4)=-\tilde{j}^2;$$

因此$-v$是$h(x)$的根. 类似地，$-w=-(\alpha_1+\alpha_4)(\alpha_2+\alpha_3)$是$h(x)$的根. 所以，

$$h(x)=(x+u)(x+v)(x+w),$$

从而

$$g(x)=(x-u)(x-v)(x-w)$$

可以从$h(x)$得到，只要改变二次项和常数项的符号. ■

命题 4.63 (i) 四次多项式$f(x) \in \mathbb{Q}[x]$的判别式$D(f)$等于它的预解三次多项式$g(x)$的判别式$D(g)$.

(ii) 如果$f(x)$不可约，则$g(x)$无重根.

证明 (i) 容易验证

$$u-v=\alpha_1\alpha_3+\alpha_2\alpha_4-\alpha_1\alpha_2-\alpha_3\alpha_4=-(\alpha_1-\alpha_4)(\alpha_2-\alpha_3).$$

类似地，$u-w=-(\alpha_1-\alpha_3)(\alpha_2-\alpha_4)$，$v-w=(\alpha_1-\alpha_2)(\alpha_3-\alpha_4)$.

由此可知$D(g)=[(u-v)(u-w)(v-w)]^2=[-\prod_{i<j}(\alpha_i-\alpha_j)]^2=D(f)$.

(ii) 如果$f(x)$是不可约的，则$f(x)$无重根（因为$\mathbb{Q}$有特征0，所以$f(x)$是可分的），从而[244] $D(f)\neq 0$. 所以$D(g)=D(f)\neq 0$，由此$g(x)$无重根. ■

用(6)式的记号，如果$f(x)$是不可约四次多项式，则u,v,w不相同.

命题 4.64 设 $f(x) \in \mathbb{Q}[x]$ 是不可约四次多项式有伽罗瓦群 G 和判别式 D，并设 m 是预解三次多项式 $g(x)$ 的伽罗瓦群的阶.

（i）如果 $m=6$，则 $G \cong S_4$. 此时，$g(x)$ 不可约且 $\sqrt{D}$ 是无理数.

（ii）如果 $m=3$，则 $G \cong A_4$. 此时，$g(x)$ 不可约且 $\sqrt{D}$ 是有理数.

（iii）如果 $m=1$，则 $G \cong \mathbf{V}$. 此时，$g(x)$ 在 $\mathbb{Q}[x]$ 中分裂.

（iv）如果 $m=2$，则 $G \cong D_8$ 或 $G \cong \mathbb{I}_4$. 此时，$g(x)$ 有一个不可约二次因式.

证明 我们已知 $E^{\mathbf{V} \cap G} = \mathbb{Q}(u, v, w)$，由伽罗瓦理论的基本定理，

$$\begin{aligned}[G : \mathbf{V} \cap G] &= [E^{\mathbf{V} \cap G} : \mathbb{Q}] \\ &= [\mathbb{Q}(u,v,w) : \mathbb{Q}] \\ &= |\operatorname{Gal}(\mathbb{Q}(u,v,w)/\mathbb{Q})| \\ &= m.\end{aligned}$$

因 $f(x)$ 不可约，由系 4.9，$|G|$ 被 4 整除，于是命题中关于群论的陈述由习题 4.28 和习题 4.29 给出. 最后，在起首两种情形中，$|G|$ 被 12 整除，命题4.59(ii)判定是 $G \cong S_4$ 还是 $G \cong A_4$. 后面两种情形中关于 $g(x)$ 的条件是容易知道的. ■

我们已经看到，对于不可约四次多项式的伽罗瓦群，由该多项式生成的预解三次多项式涉及许多内容.

例 4.65 （i）设 $f(x) = x^4 - 4x + 2 \in \mathbb{Q}[x]$. $f(x)$ 不可约［确定 $f(x)$ 不可约最好的方法是作为定理 6.34 的艾森斯坦准则，但也可用定理 3.43 确定 $f(x)$ 没有有理根，然后考察其系数的条件以证明 $f(x)$ 没有不可约二次因式］. 由命题 4.62，预解三次多项式是

$$g(x) = x^3 - 8x + 16.$$

现在 $g(x)$ 不可约（证实这个结论的最好方法还是用第 6 章中的一些结果，特别是定理 6.30，因为用 mod 5 约化可得到 $x^3 + 2x + 1$，这个多项式在 $\mathbb{I}_5$ 上不可约，因为它没有根）. $g(x)$ 的判别式是 $-4\,894$，从而定理 4.60 表明 $g(x)$ 的伽罗瓦群是 S_3，因此阶为 6. 现在定理 4.64 表明 $G \cong S_4$.

（ii）设 $f(x) = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$. 由习题6.23(viii)，$f(x)$ 不可约. 根据命题 4.62，预解三次多项式是

$$x^3 + 20x^2 + 96x = x(x+8)(x+12).$$

245

此时，$\mathbb{Q}(u,v,w) = \mathbb{Q}$ 且 $m=1$. 所以 $G \cong \mathbf{V}$.［如果回忆习题 3.122，就不会感到惊奇，在那里我们看到 $f(x)$ 是 $\alpha = \sqrt{2} + \sqrt{3}$ 的不可约多项式，其中 $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.］ ■

一个有趣的尚未解决的问题是**伽罗瓦问题的逆**：什么样的有限抽象群同构于 $\operatorname{Gal}(E/\mathbb{Q})$，其中 $E/\mathbb{Q}$ 是伽罗瓦扩张？希尔伯特证明对称群 S_n 是这种伽罗瓦群，I. Shafarevich 证明每个可解群是伽罗瓦群（见 Neukirch-Schmidt-Wingberg 所著的《Cohomology of Number Fields》）. 20 世纪 80 年代对有限群分类之后，证明大多数单群是伽罗瓦群. 更多的信息读者可参考 Malle-Matzat 所著的《Inverse Galois Theory》.

习题

4.14 证明 $\omega(1-\omega^2)(1-\omega)^2 = 3i\sqrt{3}$，其中 $\omega = e^{2\pi i/3}$.

4.15 （i）证明：如果 $a \neq 0$，则 $f(x)$ 和 $af(x)$ 的判别式相同且伽罗瓦群也相同. 由此可知，当计算伽罗瓦群时，仅关注首一多项式不会失去一般性.

(ii) 设 k 是特征 0 的域. 证明多项式 $f(x)\in k[x]$ 和它的相伴约化多项式 $\tilde{f}(x)$ 有相同的伽罗瓦群.

4.16 (i) 设 k 是特征 0 的域. 如果 $f(x)=x^3+ax^2+bx+c\in k[x]$，则它的相伴约化多项式是 x^3+qx+r，其中

$$q=b-\frac{1}{3}a^2,r=\frac{2}{27}a^3-\frac{1}{3}ab+c.$$

(ii) 证明 $f(x)$ 的判别式是

$$D=a^2b^2-4b^3-4a^3c-27c^2+18abc.$$

4.17 设 k 是域，$f(x)\in k[x]$ 是可分多项式，且 E/k 是 $f(x)$ 的分裂域. 进一步假定在 $k[x]$ 中有因式分解

$$f(x)=g(x)h(x)$$

且 B/k 和 C/k 是中间域，它们分别是 $g(x)$ 和 $h(x)$ 的分裂域.

(i) 证明 $\mathrm{Gal}(E/B)$ 和 $\mathrm{Gal}(E/C)$ 是 $\mathrm{Gal}(E/k)$ 的正规子群.

(ii) 证明 $\mathrm{Gal}(E/B)\cap\mathrm{Gal}(E/C)=\{1\}$.

(iii) 如果 $B\cap C=k$，证明 $\mathrm{Gal}(E/B)\mathrm{Gal}(E/C)=\mathrm{Gal}(E/k)$. (称中间域 B 和 C **线性无缘**，如果 $B\cap C=k$.)

(iv) 用命题 2.80 和定理 4.16 证明在这种情形下

$$\mathrm{Gal}(E/k)\cong\mathrm{Gal}(B/k)\times\mathrm{Gal}(C/k).$$

(注意 $\mathrm{Gal}(B/k)$ 不是 $\mathrm{Gal}(E/k)$ 的子群.)

246

(v) 用 (iv) 给出 $\mathrm{Gal}(E/\mathbb{Q})\cong\mathbf{V}$ 的另一个证明，其中 $E=\mathbb{Q}(\sqrt{2}+\sqrt{3})$ [见例 3.122].

(vi) 设 $f(x)=(x^3-2)(x^3-3)\in\mathbb{Q}[x]$. 如果 $B/\mathbb{Q}$ 和 $C/\mathbb{Q}$ 是 x^3-2 和 x^3-3 在 $\mathbb{C}$ 内部的分裂域，证明 $\mathrm{Gal}(E/\mathbb{Q})\ncong\mathrm{Gal}(B/\mathbb{Q})\times\mathrm{Gal}(C/\mathbb{Q})$，其中 E 是 $f(x)$ 包含在 $\mathbb{C}$ 中的分裂域.

4.18 设 k 是特征 0 的域，且 $f(x)\in k[x]$ 是有分裂域 E/k 的 5 次多项式. 证明 $f(x)$ 运用根式可解当且仅当 $[E:k]<60$.

4.19 (i) 如果 $\mathcal{L}$ 和 $\mathcal{L}'$ 是格，函数 $f:\mathcal{L}\to\mathcal{L}'$ 称为**保序的**，如果在 $\mathcal{L}$ 中 $a\leq b$ 蕴涵在 $\mathcal{L}'$ 中 $f(a)\leq f(b)$. 证明：如果 $\mathcal{L}$ 和 $\mathcal{L}'$ 是格，且 $\varphi:\mathcal{L}\to\mathcal{L}'$ 是双射满足 φ 和 φ^{-1} 都是保序的，则

$$\varphi(a\wedge b)=\varphi(a)\wedge\varphi(b),\varphi(a\vee b)=\varphi(a)\vee\varphi(b).$$

提示：修改引理 4.42 的证明.

(ii) 设 E/k 为伽罗瓦扩张，且 $\mathrm{Gal}(E/k)$ 是 n 阶循环群，证明由 $\varphi(L)=[L:k]$ 定义的

$$\varphi:\mathrm{Int}(E/k)\to\mathrm{Div}(n)$$

[见例4.40(iv)] 是保序格同构.

(iii) 证明：如果 L 和 K 是 $\mathbb{F}_{p^n}$ 的子域，则

$$[L\vee K:\mathbb{F}_p]=\mathrm{lcm}([L:\mathbb{F}_p],[K:\mathbb{F}_p])$$

和

$$[L\cap K:\mathbb{F}_p]=\gcd([L:\mathbb{F}_p],[K:\mathbb{F}_p]).$$

4.20 求子域形成链的一切有限域 k；即如果 k' 和 k'' 是 k 的子域，则 $k'\subseteq k''$ 或 $k''\subseteq k'$.

4.21 (i) 设 k 是无限域，$f(x)\in k[x]$ 是可分多项式，且 $E=k(\alpha_1,\cdots,\alpha_n)$，其中 $\alpha_1,\cdots,\alpha_n$ 是 $f(x)$ 的根. 证明存在 $c_i\in k$ 使得 $E=k(\beta)$，其中 $\beta=c_1\alpha_1+\cdots+c_n\alpha_n$.

提示：用施泰尼茨定理的证明.

(ii) (Janusz). 设 k 是有限域，且 $k(\alpha,\beta)/k$ 有限. 证明：如果 $k(\alpha)$ 和 $k(\beta)$ 线性无缘 [即如果 $k(\alpha)\cap k(\beta)=k$]，则 $E=k(\alpha+\beta)$. (该结果在一般情形下不成立. 例如，N. Boston 运用计算机代数系统 MAGMA 证明存在 $\mathbb{F}_{2^6}$ 的本原元 α 和 $\mathbb{F}_{2^{10}}$ 的本原元 β 使得 $\mathbb{F}_2(\alpha,\beta)=\mathbb{F}_{2^{30}}$，而 $\mathbb{F}_2(\alpha+\beta)=\mathbb{F}_{2^{15}}$.)

提示：用习题 4.19（ⅲ）和习题 1.26.

4.22 设 E/k 是伽罗瓦扩张有伽罗瓦群 $G=\mathrm{Gal}(E/k)$．定义迹 $T: E\to E$ 为

$$T(u)=\sum_{\sigma\in G}\sigma(u).$$

（ⅰ）证明 $\mathrm{im}T\subseteq k$ 且对一切 $u,v\in E$，$T(u+v)=T(u)+T(v)$．

（ⅱ）用特征标的无关性证明 T 不恒为零.

4.23 设 E/k 是伽罗瓦扩张，且有 $[E:k]=n$ 及循环伽罗瓦群 $G=\mathrm{Gal}(E/k)$，比如 $G=\langle\sigma\rangle$．定义 $\tau=\sigma-1_E$，证明 $\ker T=\mathrm{im}\tau$，其中 $T: E\to E$ 是迹.由此推出，在这种情形下，迹定理成立：

$$\ker T=\{a\in E:\text{对某个 } u\in E \text{ 有 } a=\sigma(u)-u\}.$$

提示：证明 $\ker\tau=k$，从而 $\dim(\mathrm{im}\tau)=n-1=\dim(\ker T)$.

247

4.24 设 k 是特征 $p>0$ 的域，且 E/k 是有 p 阶循环伽罗瓦群 $G=\langle\sigma\rangle$ 的伽罗瓦扩张．用迹定理证明存在一个元素 $u\in E$ 使得 $\sigma(u)-u=1$．证明 $E=k(u)$ 且存在 $c\in k$ 使得 $\mathrm{irr}(u,k)=x^p-x-c$.

4.25 如果 $\sigma\in S_n$ 且 $f(x_1,\cdots,x_n)\in k[x_1,\cdots,x_n]$，其中 k 是域，定义

$$(\sigma f)(x_1,\cdots,x_n)=f(x_{\sigma1},\cdots,x_{\sigma n}).$$

（ⅰ）证明 $(\sigma,f(x_1,\cdots,x_n))\mapsto\sigma f$ 定义了 S_n 在 $k[x_1,\cdots,x_n]$ 上的一个作用.

（ⅱ）设 $\Delta=\Delta(x_1,\cdots,x_n)=\prod_{i<j}(x_i-x_j)$（在 239 页上，我们知道对一切 $\sigma\in S_n$，$\sigma\Delta=\pm\Delta$）．如果 $\sigma\in S_n$，证明 $\sigma\in A_n$ 当且仅当 $\sigma\Delta=\Delta$.

提示：定义 $\varphi: S_n\to G$ 为

$$\varphi(\sigma)=\begin{cases}1 & \text{当 } \sigma\Delta=\Delta;\\ -1 & \text{当 } \sigma\Delta=-\Delta,\end{cases}$$

其中 G 是乘法群 $\{1,-1\}$．证明 φ 是同态且 $\ker\varphi=A_n$.

4.26 证明：如果 $f(x)\in\mathbb{Q}[x]$ 是不可约四次多项式，它的判别式有有理平方根，则 $f(x)$ 的伽罗瓦群的阶为 4 或 12.

4.27 设 $f(x)=x^4+rx+s\in\mathbb{Q}[x]$ 有伽罗瓦群 G.

（ⅰ）证明 $f(x)$ 的判别式是 $-27r^4+256s^3$.

（ⅱ）证明：如果 $s<0$，则 G 不同构于 A_4 的子群.

（ⅲ）证明 $f(x)=x^4+x+1$ 不可约且 $G\cong S_4$.

4.28 设 G 是 S_4 的子群且 $|G|$ 是 4 的倍数，定义 $m=|G/(G\cap\mathbf{V})|$.

（ⅰ）证明 m 是 6 的因数.

（ⅱ）如果 $m=6$，则 $G=S_4$；如果 $m=3$，则 $G=A_4$；如果 $m=1$，则 $G=\mathbf{V}$；如果 $m=2$，则 $G\cong D_8$，$G\cong\mathbb{I}_4$ 或 $G\cong\mathbf{V}$.

4.29 设 G 是 S_4 的子群．如果 G 传递地作用在 $X=\{1,2,3,4\}$ 上，且 $|G/(\mathbf{V}\cap G)|=2$，则 $G\cong D_8$ 或 $G\cong\mathbb{I}_4$．[如果我们仅仅假定 G 传递地作用在 X 上，则 $|G|$ 是 4 的倍数（系 4.9)．附加的假设 $|G/(\mathbf{V}\cap G)|=2$ 排除了习题 4.28 中当 $m=2$ 时 $G\cong\mathbf{V}$ 的可能性.]

4.30 计算$\mathbb{Q}$上 x^4+x^2-6 的伽罗瓦群.

4.31 计算$\mathbb{Q}$上 $f(x)=x^4+x^2+x+1$ 的伽罗瓦群.

提示：用例3.35(ⅱ)证明 $f(x)$ 的不可约性，并用 mod 2 约化证明预解三次多项式的不可约性.

4.32 计算$\mathbb{Q}$上 $f(x)=4x^4+12x+9$ 的伽罗瓦群.

提示：分两步证明 $f(x)$ 不可约：先证明 $f(x)$ 没有有理根，然后用笛卡儿（Descartes）方法（209 页）证明 $f(x)$ 不是$\mathbb{Q}$上两个二次多项式的积.

248

第5章 群 Ⅱ

我们现在探索有关群的结构的一些信息. 有限阿贝尔群不太复杂：它们是循环群的直和. 回到非阿贝尔群，西罗定理证明，对任意素数 p，有限群 G 有 p^e 阶子群，其中 p^e 是整除 $|G|$ 的 p 的最大幂，且任意两个这样的群同构. 在伽罗瓦理论中引发的正规列和可解性的思想产生了群的不变量（若尔当-赫尔德定理），它表明单群在某种意义上是建造有限群的“砖块”. 随后，我们展示了更多单群的例子来伴随交错群 A_n，对 $n\geqslant 5$，我们已经证明 A_n 是单群. 本章终止于自由群和群表现的研究，因为它们在构造和描述任意群中是有用的，本章结尾证明每个自由群的子群也是自由群.

5.1 有限阿贝尔群

我们通过对一切有限阿贝尔群进行分类来继续群的研究；遵循习惯，对于这些群中的二元运算使用加法记号. 我们要证明每个有限阿贝尔群都是循环群的直和且在很强的意义下，这种分解是唯一的.

5.1.1 直和

本小节中的群是指任意的可以是无限的阿贝尔群.

有两种方式描述阿贝尔群 S_1，…，S_n 的直和. 最简单的方式有时候称为**外直和**，记为 $S_1\times\cdots\times S_n$，它的元素是 n 元组$(s_1,\cdots,s_n)$，其中对一切 i，$s_i\in S_i$，它的二元运算是

$$(s_1,\cdots,s_n)+(s_1',\cdots,s_n')=(s_1+s_1',\cdots,s_n+s_n').$$

然而最有用的方式有时称为**内直和**，它同构于 $S_1\times\cdots\times S_n$，涉及满足 $G\cong S_1\times\cdots\times S_n$ 的给定的群 G 的子群 S_i. 我们常省略形容词外和内.

两个子群的直和的定义就是用加法来陈述命题 2.80.

定义 设 S 和 T 都是阿贝尔群 G 的子群. 如果 $S+T=G$（即对每个 $a\in G$，存在 $s\in S$ 和 $t\in T$ 使得 $a=s+t$）且 $S\cap T=\{0\}$，则称 G 是**直和**，记为

$$G=S\oplus T.$$

下面是直和的几个特征.

命题5.1 对阿贝尔群 G 和它的子群 S，T，下列陈述等价.

(ⅰ) $G=S\oplus T$.

(ⅱ) 每个 $g\in G$ 有形如

$$g=s+t$$

的唯一表达式，其中 $s\in S$，$t\in T$.

(ⅲ) 存在称为**投射**的同态 $p:G\to S$ 和 $q:G\to T$，以及称为**内射**的同态 $i:S\to G$ 和 $j:T\to G$ 满足

$$pi=1_S,qj=1_T,pj=0,qi=0 和 ip+jq=1_G.$$

注 等式 $pi=1_S$ 和 $qj=1_T$ 蕴涵映射 i 和 j 必是单射且 p 和 q 必是满射.

证明 (i) ⇒ (ii). 由假设, $G=S+T$, 从而每个 $g\in G$ 有形如 $g=s+t$ 的表达式, 其中 $s\in S$, $t\in T$. 为证明这个表达式唯一, 假定还有 $g=s'+t'$, 其中 $s'\in S$, $t'\in T$. 则 $s+t=s'+t'$ 给出 $s-s'=t'-t\in S\cap T=\{0\}$. 所以正如所要的 $s=s'$ 和 $t=t'$.

(ii) ⇒ (iii). 如果 $g\in G$, 则存在唯一的 $s\in S$, $t\in T$ 使得 $g=s+t$. 定义函数 p 和 q 为

$$p(g)=s \quad 和 \quad q(g)=t,$$

由于唯一性的假设, p, q 是合理定义的. 容易验证 p, q 是同态且陈述中的所有等式成立.

(iii) ⇒ (i). 如果 $g\in G$, 因为 $S=\operatorname{im} i$ 和 $T=\operatorname{im} j$, 等式 $1_G=ip+jq$ 给出

$$g=ip(g)+jq(g)\in S+T.$$

250

如果 $g\in S$, 则 $g=ig$ 且 $pg=pig=g$; 如果 $g\in T$, 则 $g=jg$ 且 $pg=pig=0$. 所以, 如果 $g\in S\cap T$, 则 $g=0$. 因此 $S\cap T=\{0\}$, $S+T=G$, 从而 $G=S\oplus T$. ■

下一结果表明内直和和外直和之间没有本质的差别.

系 5.2 设 S 和 T 是阿贝尔群 G 的子群. 如果 $G=S\oplus T$, 则 $S\oplus T\cong S\times T$.

反之, 给定阿贝尔群 S 和 T, 定义 $S\times T$ 的子群 $S'\cong S$ 和 $T'\cong T$ 为

$$S'=\{(s,0):s\in S\} \quad 和 \quad T'=\{(0,t):t\in T\},$$

则 $S\times T=S'\oplus T'$.

证明 定义 $f:S\oplus T\to S\times T$ 如下. 如果 $a\in S\oplus T$, 则命题 5.1 说存在形如 $a=s+t$ 的唯一表达式, 从而 $f:a\mapsto(s,t)$ 是合理定义的函数. 容易验证 f 是同构.

反之, 如果 $g=(s,t)\in S\times T$, 则 $g=(s,0)+(0,t)\in S'+T'$ 且 $S'\cap T'=\{(0,0)\}$. 因此 $S\times T=S'\oplus T'$. ■

定义 如果 S_1, S_2, …, S_n, …是阿贝尔群 G 的子群, 对 $n\geqslant 2$ 归纳定义**有限直和** $S_1\oplus S_2\oplus\cdots\oplus S_n$:

$$S_1\oplus S_2\oplus\cdots\oplus S_{n+1}=[S_1\oplus S_2\oplus\cdots\oplus S_n]\oplus S_{n+1}.$$

这个直和也记为

$$\sum_{i=1}^{n}S_i=S_1\oplus S_2\oplus\cdots\oplus S_n.$$

给定阿贝尔群 G 的子群 S_1, S_2, …, S_n, 什么时候这些子群生成的群 $\langle S_1,S_2,\cdots,S_n\rangle$ 等于它们的直和? 一个常犯的错误是认为只要假定对一切 $i\neq j$ 有 $S_i\cap S_j=\{0\}$ 就可以了, 但下面的例子表明这是不够的.

例 5.3 设 V 是域 k 上的二维向量空间, 我们把它看作加法阿贝尔群, 并设 x, y 是基. 容易验证子群 $\langle x\rangle$, $\langle y\rangle$ 和 $\langle x+y\rangle$ 中的任两个的交是 $\{0\}$. 另一方面, 因为 $[\langle x\rangle\oplus\langle y\rangle]\cap\langle x+y\rangle\neq\{0\}$, 所以 $V=[\langle x\rangle\oplus\langle y\rangle]\oplus\langle x+y\rangle$ 不成立. ■

在有关阿贝尔群的上下文中, 我们将用 $S\subseteq G$ 表示 S 是 G 的子群, 如同子环和理想所用的记号. 对于一般的群, (可以是非阿贝尔群) 我们继续用 $S\leqslant G$ 表示子群.

251

命题 5.4 设 $G=S_1+S_2+\cdots+S_n$, 其中 S_i 是子群; 即对每个 $a\in G$, 关于一切 i, 存在 $s_i\in S_i$ 使得

$$a=s_1+s_2+\cdots+s_n.$$

则下面的条件等价:

(i) $G=S_1\oplus S_2\oplus\cdots\oplus S_n$.

(ii) 每个 $a\in G$ 都有唯一的形如 $a=s_1+s_2+\cdots+s_n$ 的表达式，其中对一切 i，$s_i\in S_i$.

(iii) 对每个 i，

$$S_i\cap(S_1+S_2+\cdots+\hat{S}_i+\cdots+S_n)=\{0\},$$

其中 $\hat{S}_i$ 表示从和式中删除 S_i 这一项.

证明 (i) ⇒ (ii). 对 $n\geqslant 2$ 用归纳法证明. 基础步是命题 5.1. 关于归纳步，定义 $T=S_1+S_2+\cdots+S_n$，从而 $G=T\oplus S_{n+1}$. 如果 $a\in G$，则 a 有唯一的形如 $a=t+s_{n+1}$ 的表达式，其中 $t\in T$，$s_{n+1}\in S_{n+1}$ (根据命题). 但归纳假设说 t 有唯一的形如 $t=s_1+s_2+\cdots+s_n$ 的表达式，其中对一切 $i\leqslant n$，$s_i\in S_i$，这正是所要的结果.

(ii) ⇒ (iii). 假设

$$x\in S_i\cap(S_1+S_2+\cdots+\hat{S}_i+\cdots+S_n).$$

则 $x=s_i\in S_i$ 且 $s_i\in\sum_{j\neq i}s_j$，其中 $s_j\in S_j$. 除非所有的 $s_j=0$，否则元素 0 有两个不同的表达式：$0=-s_i+\sum_{j\neq i}s_j$ 和 $0=0+0+\cdots+0$. 所以一切 $s_j=0$ 且 $x=s_i=0$.

(iii) ⇒ (i). 因 $S_{n+1}\cap(S_1+S_2+\cdots+S_n)=\{0\}$，有

$$G=S_{n+1}\oplus(S_1+S_2+\cdots+S_n).$$

因为对一切 $j\leqslant n$，有

$$S_j\cap(S_1+\cdots+\hat{S}_j+\cdots+S_n)\subseteq S_j\cap(S_1+\cdots+\hat{S}_j+\cdots+S_n+S_{n+1})=\{0\}.$$

因此归纳假设给出 $S_1+S_2+\cdots+S_n=S_1\oplus S_2\oplus\cdots\oplus S_n$. ■

系 5.5 设 $G=\langle y_1,\cdots,y_n\rangle$. 如果对一切 $m_i\in\mathbb{Z}$，$\sum_i m_iy_i=0$ 蕴涵 $m_iy_i=0$，则

$$G=\langle y_1\rangle\oplus\cdots\oplus\langle y_n\rangle.$$

证明 由命题5.4(ii)，只需证明如果 $\sum_i k_iy_i=\sum_i \ell_iy_i$，则对一切 i，$k_iy_i=\ell_iy_i$. 而这是显然的，因为 $\sum_i(k_i-\ell_i)y_i=0$ 蕴涵对一切 i 有 $(k_i-\ell_i)y_i=0$. ■

252

例 5.6 设 V 是域 k 上的 n 维向量空间，我们把它看作加法阿贝尔群. 如果 v_1，…，v_n 是基，则

$$V=\langle v_1\rangle\oplus\langle v_2\rangle\oplus\cdots\oplus\langle v_n\rangle,$$

其中 $\langle v_i\rangle=\{rv_i:r\in k\}$ 是由 v_i 张成的一维子空间. 因为 v_1，…，v_n 是基，所以每个 $v\in V$ 有形如 $v=s_1+\cdots+s_n$ 的唯一表达式，其中 $s_i=r_iv_i\in\langle v_i\rangle$. ■

现在我们已经考察了有限直和，可以把命题 2.79 从两个直和项推广到有限个直和项. 虽然我们的结果是对阿贝尔群说的，但应该明白如果假设子群 H_i 是正规子群，则对非阿贝尔群也可以作同样的论证 (见习题 5.1).

命题 5.7 如果 G_1，G_2，…，G_n 是阿贝尔群且 $H_i\subseteq G_i$ 是子群，则

$$(G_1\oplus\cdots\oplus G_n)/(H_1\oplus\cdots\oplus H_n)\cong(G_1/H_1)\times\cdots\times(G_n/H_n).$$

证明 定义 $f:G_1\oplus\cdots\oplus G_n\to(G_1/H_1)\oplus\cdots\oplus(G_n/H_n)$ 为

$$(g_1,\cdots,g_n)\mapsto(g_1+H_1,\cdots,g_n+H_n).$$

因 f 是满同态满足 $\ker f=H_1\oplus\cdots\oplus H_n$，第一同构定理给出结论. ■

如果 G 是阿贝尔群，m 是整数，记

$$mG = \{ma : a \in G\}.$$

易知 mG 是 G 的子群.

命题 5.8 如果 G 是阿贝尔群且 p 是素数，则 G/pG 是 $\mathbb{F}_p$ 上的向量空间.

证明 如果 $[r] \in \mathbb{F}_p$ 且 $a \in G$，定义标量乘法

$$[r](a + pG) = ra + pG.$$

这个公式是合理定义的，因为如果 $k \equiv r \bmod p$，则对某个整数 m 有 $k = r + pm$，由于 $pma \in pG$，因此

$$ka + pG = ra + pma + pG = ra + pG,$$

现在容易验证向量空间的公理都成立. ■ 253

$\mathbb{Z}$ 的复制的直和经常出现，从而需要它们自己的名称.

定义 设 $F = \langle x_1, \cdots, x_n \rangle$ 是阿贝尔群. 如果

$$F = \langle x_1 \rangle \oplus \cdots \oplus \langle x_n \rangle,$$

其中每个 $\langle x_i \rangle \cong \mathbb{Z}$，则称 F 为（有限生成的）以 x_1，…，x_n 为基的**自由阿贝尔群**. 更一般地，称任意一个同构于 F 的群为自由阿贝尔群.

例如，$\mathbb{Z}^m = \mathbb{Z} \times \cdots \times \mathbb{Z}$ 是整数的一切 m 元组 $(n_1, \cdots, n_m)$ 组成的群，是一个自由阿贝尔群.

命题 5.9 如果 $\mathbb{Z}^m$ 表示 $\mathbb{Z}$ 的 m 个复制的直和，则 $\mathbb{Z}^m \cong \mathbb{Z}^n$ 当且仅当 $m = n$.

证明 只有必要性需要证明. 首先注意对任意阿贝尔群 G，如果 $G = G_1 \oplus \cdots \oplus G_n$，则 $2G = 2G_1 \oplus \cdots \oplus 2G_n$. 由命题 5.7，

$$G/2G \cong (G_1/2G_1) \oplus \cdots \oplus (G_n/2G_n),$$

从而如果 $G = \mathbb{Z}^n$，则 $|G/2G| = 2^n$. 类似地，如果 $H = \mathbb{Z}^m$，则 $|H/2H| = 2^m$. 最后，如果 $G = \mathbb{Z}^n \cong \mathbb{Z}^m = H$，则 $G/2G \cong H/2H$，从而 $2^n = 2^m$. 由此可知 $n = m$. ■

系 5.10 如果 F 是（有限生成的）自由阿贝尔群，则 F 的任两个基的元素个数相等.

证明 如果 x_1，…，x_n 是 F 的基，则 $F \cong \mathbb{Z}^n$. 如果 y_1，…，y_m 是 F 的另一组基，则 $F \cong \mathbb{Z}^m$. 由命题，$m = n$. ■

定义 如果 F 是以 $x_1, \cdots, x_n$ 为基的自由阿贝尔群，则称 n 为 F 的**秩**，记为 $\text{rank}(F) = n$.

系 5.10 说明 $\text{rank}(F)$ 是合理定义的；即它不依赖于基的选取. 运用这个定义，命题 5.9 说两个有限生成的自由阿贝尔群同构当且仅当它们有相同的秩；即自由阿贝尔群的秩扮演了向量空间的维数的角色. 把下一定理和定理 3.92 相比较，说明自由阿贝尔群的基和向量空间的基有相同的性态.

定理 5.11 设 F 是以 $X = \{x_1, \cdots, x_n\}$ 为基的自由阿贝尔群. 如果 G 是任意一个阿贝尔群且 $\gamma : X \to G$ 是任意函数，则存在唯一的同态 $g : F \to G$ 使得对一切 x_i，$g(x_i) = \gamma(x_i)$.

$$\begin{array}{ccc} F & & \\ \uparrow & \searrow^{g} & \\ X & \xrightarrow{\gamma} & G \end{array}$$

证明 每个元素 $a \in F$ 有形如 254

$$a = \sum_{i=1}^{n} m_i x_i$$

的唯一表达式，其中 $m_i \in \mathbb{Z}$. 定义 $g : F \to G$ 为

$$g(a)=\sum_{i=1}^{n} m_i\gamma(x_i).$$

如果 $h: F\to G$ 是同态使得对一切 $i, h(x_i)=g(x_i)$，则 $h=g$，这是因为在生成元的集合上一致的两个同态必相等. ■

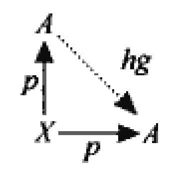
定理 5.11 刻画了自由阿贝尔群.

命题 5.12 设 A 是包含子集 $X=\{x_1,\cdots,x_n\}$ 的阿贝尔群，并设 A 具有定理 5.11 中的性质：对每个阿贝尔群 G 和每个函数 $\gamma: X\to G$，存在唯一的同态 $g: A\to G$ 使得对一切 $x_i, g(x_i)=\gamma(x_i)$，则 $A\cong \mathbb{Z}^n$；即 A 是秩为 n 的自由阿贝尔群.

证明 考虑图

和

其中 $p: X\to A$ 和 $q: X\to \mathbb{Z}^n$ 是包含函数. 第一个图来自给定的 A 的性质，因此 $gp=q$. 第二个图来自定理 5.11，它表明 $\mathbb{Z}^n$ 具有同样的性质，因此 $hq=p$. 我们断言映射 $g: A\to \mathbb{Z}^n$ 是同构. 为此，考虑图



现在 $hgp=hq=p$. 由假设，hg 是唯一的这种同态，而 1_A 是另一个这种同态，从而 $hg=1_A$. 类似的图表明另一个复合 $gh=1_{\mathbb{Z}^n}$，从而 g 是同构. ■

5.1.2 基定理

用"一次一个素数"的方式来分析有限阿贝尔群是方便的.

回忆 p-群是对某个 $k\geq 0$ 的 p^k 阶有限群 G. 在专门研究阿贝尔群的上下文中，称 p-群为 p-准素群.

255

定义 如果 p 是素数，则阿贝尔群 G 称为 **p-准素群**，如果对每个 $a\in G$，存在 $n\geq 1$ 使得 $p^n a=0$. 如果 G 是任意阿贝尔群，则它的 **p-准素分量**是

$$G_p=\{a\in G: 对某个\ n\geq 1, p^n a=0\}.$$

易知对每个素数 p，G_p 是 G 的子群（当 G 不是阿贝尔群时不成立，例如如果 $G=S_3$，则 G_2 不是它的子群).

如果我们并不需要指定素数 p，则可以记一个阿贝尔群为准素群（而不是 p-准素群).

定理 5.13（准素分解） （ⅰ）每个有限阿贝尔群都是它的 p-准素分量的直和：

$$G=G_{p_1}\oplus\cdots\oplus G_{p_n}.$$

（ⅱ）两个有限阿贝尔群 G 和 G' 同构当且仅当对每个素数 p，$G_p\cong G'_p$.

证明 （ⅰ）设 $x\in G$ 非零，并设它的阶为 d. 由算术基本定理，存在不同的素数 $p_1,\cdots,p_n$ 和正指数 $e_1,\cdots,e_n$ 使得

$$d=p_1^{e_1}\cdots p_n^{e_n}.$$

定义 $r_i=d/p_i^{e_i}$，从而 $p_i^{e_i}r_i=d$. 由此对每个 i，$r_ix\in G_{p_i}$（因为 $dx=0$). 而 r_1，…，r_n 的 gcd$d$ 是

1（d 的可能的素因数只有 $p_1,\cdots,p_n$，但因 $p_i\nmid r_i$，所以没有一个 p_i 是公因数），因此存在整数 $s_1,\cdots,s_n$ 使得$1=\sum_i s_ir_i$．所以，

$$x=\sum_i s_ir_ix\in G_{p_1}+\cdots+G_{p_n}. \quad \bullet$$

记 $H_i=G_{p_1}+G_{p_2}+\cdots+\hat{G}_{p_i}+\cdots+G_{p_n}$．由命题 5.4，只需证明如果

$$x\in G_{p_i}\cap H_i,$$

则 $x=0$．因 $x\in G_{p_i}$，对某个 $\ell\geqslant 0$，有 $p_i^{\ell}x=0$．因 $x\in H_i$，有 $x=\sum_{j\neq i}y_j$，其中 $p_j^{g_j}y_j=0$．因此 $ux=0$,其中 $u=\prod_{j\neq i}p_j^{g_j}$．而 p_i^{ℓ} 和 u 互素，从而存在整数 s 和 t 使得 $1=sp_i^{\ell}+tu$．所以，

$$x=(sp_i^{\ell}+tu)x=sp_i^{\ell}x+tux=0.$$

（ii）如果 $f:G\to G'$是同态,则对每个素数 p，因为 $p^{\ell}a=0$ 导出 $0=f(p^{\ell}a)=p^{\ell}f(a)$，所以 $f(G_p)\subseteq G'_p$．如果 f 是同构，则 $f^{-1}:G'\to G$ 也是同构[从而对一切 p, $f^{-1}(G'_p)\subseteq G_p$]．由此，每个限制 $f\mid G_p:G_p\to G'_p$ 是同构,有逆 $f^{-1}\mid G'_p$.

反之，如果对一切 p 存在同构 $f_p:G_p\to G'_p$，则由 $\sum_p a_p\mapsto\sum_p f_p(a_p)$ 给出同构 $\varphi:\sum_p G_p\to\sum_p G'_p$．■ [256]

下面类型的子群将扮演一个重要角色.

定义 设 p 是素数，G 是 p-准素阿贝尔群⊖．子群 $S\subseteq G$ 称为**纯**⊜**子群**，如果对一切 $n\geqslant 0$，

$$S\cap p^nG=p^nS.$$

包含关系 $S\cap p^nG\geqslant p^nS$ 对每个子群 $S\subseteq G$ 都成立，从而只有反包含 $S\cap p^nG\subseteq p^nS$ 是重要的．它是说如果 $s\in S$ 对某个 $a\in G$ 满足等式 $s=p^na$，则存在 $s'\in S$ 使得$s=p^ns'$.

例 5.14 （i）G 的每个直和项 S 都是纯子群．如果 $G=S\oplus T$ 且 $(s,0)=p^n(u,v)$，其中 $u\in S$，$v\in T$，则显然有 $(s,0)=p^n(u,0)$．（逆命题："每个纯子群都是一个直和项"当 S 有限时成立，当 S 无限时可能不成立.）

（ii）如果 $G=\langle a\rangle$ 是 p^2 阶循环群，其中 p 是素数，则 $S=\langle pa\rangle$ 不是 G 的纯子群，这是因为如果 $s=pa\in S$，则不存在元素 $s'\in S$ 使得 $s=pa=ps'$．■

引理 5.15 如果 p 是素数且 G 是有限 p-准素阿贝尔群，则 G 有非零的纯循环子群.

证明 因 G 有限，可以选取阶最大的元素 $y\in G$，比如阶为 p^{ℓ}．我们断言 $S=\langle y\rangle$ 是 G 的纯子群.

假设 $s\in S$，从而 $s=mp^ty$，其中 $t\geqslant 0$ 且 $p\nmid m$，并设对某个 $a\in G$ 有

$$s=p^na.$$

必能找到元素 $s'\in S$ 使得 $s=p^ns'$．可假定 $n<\ell$，否则 $s=p^na=0$（因为 y 有最大阶 p^{ℓ}，所以对一切 $g\in G,p^{\ell}g=0$），可取 $s'=0$.

如果 $t\geqslant n$，定义 $s'=mp^{t-n}y\in S$，注意

$$p^ns'=p^nmp^{t-n}y=mp^ty=s.$$

⊖ 如果 G 不是准素群，则定义纯子群 $S\subseteq G$ 为对一切 $m\in\mathbb{Z}$，满足 $S\cap mG=mS$ 的子群（见习题 5.2 和习题 5.3).

⊜ 回忆在讨论运用根式可解性的时候产生了纯扩张 $k(u)/k$．在这种扩张中，添加的元素 u 对某个 $a\in k$ 满足等式 $u^n=a$．纯子群由类似的等式定义（用加法记号），可能这就是其名称的由来.

如果 $t<n$，则

$$p^{\ell}a = p^{\ell-n}p^{n}a = p^{\ell-n}s = p^{\ell-n}mp^{t}y = mp^{\ell-n+t}y.$$

但 $p\nmid m$，且因 $-n+t<0$，所以 $\ell-n+t<\ell$，从而 $p^{\ell}a\neq 0$. 这与 y 有最大阶矛盾，因此这种情形
257 不可能出现. ■

定义 如果 p 是素数，G 是有限 p-准素阿贝尔群，则

$$d(G) = \dim(G/pG).$$

注意到 d 在直和上可加，

$$d(G\oplus H) = d(G)+d(H),$$

这是因为命题 2.79 给出

$$(G\oplus H)/p(G\oplus H) = (G\oplus H)/(pG\oplus pH)$$
$$\cong (G/pG)\oplus(H/pH).$$

左端的维数是 $d(G\oplus H)$. 因为 G/pG 的基和 H/pH 的基的并是 $(G/pG)\oplus(H/pH)$ 的基，所以右端的维数是 $d(G)+d(H)$.

容易刻画 $d(G)=1$ 的非零阿贝尔群 G.

引理 5.16 如果 $G\neq\{0\}$ 是 p-准素的，则 $d(G)=1$ 当且仅当 G 是循环群.

证明 如果 G 是循环群，则 G 的任一商群也是循环群，特别是 G/pG 是循环群，因此 $\dim(G/pG)=1$.

反之，如果 $G/pG=\langle z+pG\rangle$，则 $G/pG\cong\mathbb{I}_p$. 因 $\mathbb{I}_p$ 是单群，对应定理说 pG 是 G 的极大真子群，我们断言 G 只有 pG 这一个极大真子群. 如果 $L\subseteq G$ 是任意一个极大真子群，因为 G/L 是单阿贝尔群，阶为 p 的幂，因此阶是 p，所以 $G/L\cong\mathbb{I}_p$（根据命题 2.107，阿贝尔单群都是素数阶循环群）. 于是，如果 $a\in G$，则在 G/L 中 $p(a+L)=0$，从而 $pa\in L$，因此 $pG\subseteq L$. 而 pG 是极大的，所以 $pG=L$. 由此，G 的每个真子群都包含在 pG 中（因为每个真子群都包含在某个极大真子群中）. 特别地，如果 $\langle z\rangle$ 是 G 的真子群，则 $\langle z\rangle\subseteq pG$，与 $z+pG$ 是 G/pG 的生成元矛盾. 所以 $G=\langle z\rangle$，从而 G 是循环群. ■

引理 5.17 设 G 是有限 p-准素阿贝尔群.

（i）如果 $S\subseteq G$，则 $d(G/S)\leqslant d(G)$.

（ii）如果 S 是 G 的纯子群，则

$$d(G) = d(S)+d(G/S).$$

证明 （i）由对应定理，$p(G/S)=(pG+S)/S$，因此由第三同构定理，

$$(G/S)/p(G/S) = (G/S)/[(pG+S)/S]\cong G/(pG+S).$$

因 $pG\subseteq pG+S$，存在满同态（$\mathbb{F}_p$ 上向量空间的同态），
258
$$G/pG\to G/(pG+S),$$

也就是 $g+pG\mapsto g+(pG+S)$. 因此 $\dim(G/pG)\geqslant\dim(G/(pG+S))$，即 $d(G)\geqslant d(G/S)$.

（ii）我们现在分析 $(pG+S)/pG$，即 $G/pG\to G/(pG+S)$ 的核. 由第二同构定理，

$$(pG+S)/pG\cong S/(S\cap pG).$$

因 S 是纯子群，故 $S\cap pG=pS$，所以，

$$(pG+S)/pG\cong S/pS,$$

从而 $\dim[(pG+S)/pG]=d(S)$. 但如果 W 是有限维向量空间 V 的子空间，则由习题 3.72，

$\dim(V) = \dim(W) + \dim(V/W)$. 因此，如果 $V=G/pG$ 和 $W = (pG+S)/pG$，则有

$$d(G) = d(S) + d(G/S).$$ ■

定理 5.18 (基定理) 每个有限阿贝尔群都是阶为素数幂的循环群的直和.

证明 由定理 5.13 的准素分解，可以假定 G 是关于某个素数 p 的 p-准素群. 对 $d(G) \geqslant 1$ 用归纳法证明 G 是循环群的直和. 容易验证基础步，因为引理 5.16 证明此时 G 必是循环群.

为证明归纳步，我们先用引理 5.15 找出一个非零纯循环子群 $S\subseteq G$. 根据引理 5.17，有

$$d(G/S) = d(G) - d(S) = d(G) - 1 < d(G).$$

由归纳假设，G/S 是循环群的直和，比如

$$G/S = \sum_{i=1}^{q} \langle \bar{x}_i \rangle,$$

其中 $\bar{x}_i = x_i + S$.

设 $x\in G$ 并设 $\bar{x}$ 的阶为 p^ℓ，其中 $\bar{x}=x+S$. 我们断言存在 $z\in G$ 使得 $z+S=\bar{x}=x+S$ 满足

$$\text{阶 } z = \text{阶}(\bar{x}).$$

现在 x 的阶为 p^n，其中 $n\geqslant \ell$. 但在 G/S 中 $p^\ell(x+S) = p^\ell \bar{x} = 0$，因此存在某个 $s\in S$ 使得 $p^\ell x = s$. 由纯性，存在 $s'\in S$ 使得 $p^\ell x = p^\ell s'$. 如果定义 $z = x - s'$，则 $p^\ell z = 0$ 且 $z+S = x+S = \bar{x}$. 如果 z 的阶为 p^m，则因为 $z \mapsto \bar{x}$，所以有 $m \geqslant \ell$. 因 $p^\ell z = 0$，所以 z 的阶等于 p^ℓ.

对每个 i，选取 $z_i\in G$ 使得 $z_i + S = \bar{x}_i = x_i + S$ 且阶 z_i = 阶 $\bar{x}_i$. 定义 T 为

$$T = \langle z_1, \cdots, z_q \rangle.$$

259

因为 G 由 S 和各 z_i 生成，所以 $S+T=G$. 为证明 $G=S\oplus T$，现在只需证明 $S\cap T=\{0\}$. 如果 $y\in S\cap T$，则 $y = \sum_i m_i z_i$，其中 $m_i\in\mathbb{Z}$. 现在 $y\in S$，于是在 G/S 中 $\sum_i m_i \bar{x}_i = 0$. 由于这是一个直和，所以每个 $m_i\bar{x}_i = 0$. 终究，对每个 i，

$$-m_i\bar{x}_i = \sum_{j\neq i} m_j \bar{x}_j \in \langle \bar{x}_i \rangle \cap (\langle \bar{x}_1 \rangle + \cdots + \widehat{\langle \bar{x}_i \rangle} + \cdots + \langle \bar{x}_q \rangle) = \{0\}.$$

所以对一切 i，$m_i z_i = 0$，因此 $y=0$.

最后，$G=S\oplus T$ 蕴涵 $d(G) = d(S) + d(T) = 1 + d(T)$，因此 $d(T) < d(G)$. 由归纳假设，T 是循环群的直和，证明完成. ■

我所知道的这个基定理的最短的证明属于 G. Navarro，*American Mathematical Monthly*，110 (2003)，153～154 页.

引理 5.19 有限 p-准素阿贝尔群 G 是循环群当且仅当它有唯一的 p 阶子群.

证明 回忆 94 页未编号的定理：如果 G 是 n 阶阿贝尔群，且对 n 的每个素因数 p，至多有一个 p 阶循环子群，则 G 是循环群. 当 n 是 p 的幂时，可立刻得到本引理. 逆命题是引理 2.85. ■

注 我们不能删除 G 是阿贝尔群的假设，因为四元数群 $\mathbf{Q}$ 是 2-群，它有唯一的 2 阶子群. 然而，如果 G 是有限 p-群（可以是非阿贝尔群），它有唯一的 p 阶子群，则 G 或者是循环群，或者是广义四元数群（广义四元数群的定义在 298 页）. 这个结果的证明可以在 Rotman 所著的《An Introduction to the Theory of Groups》121～122 页上找到.

有限性的假设是不能删除的，因为命题9.25(ⅲ)表明无限 p-准素群$\mathbb{Z}(p^\infty)$ 有唯一的 p 阶子群.

引理 5.20 如果 G 是有限 p-准素阿贝尔群且 a 是 G 中阶最大的元素，则 $A=\langle a\rangle$ 是 G 的直和项.

证明 对 $|G|\geqslant 1$ 用归纳法证明. 基础步显然成立. 可以假定 G 不是循环群，因为任意一个群都是它自身的直和项（余下的直和项是$\{0\}$）. 现在 A 有唯一的 p 阶子群，把它叫做 C. 根据引理 5.19，G 包含另一个 p 阶子群，比如 C'. 当然 $A\cap C'=\{0\}$. 根据第二同构定理，$(A+C')/C'\cong A/(A\cap C')\cong A$ 是 G/C' 的循环子群. 但 G 的同态象不能有阶大于 $|A|$ 的循环子群（因为象中元素的阶不能大于 a 的阶）. 所以，$(A+C')/C'$ 是 G/C' 中阶最大的子群，由归纳假设，它是直和项：存在子群 B/C' 使得

$$G/C'=((A+C')/C')\oplus(B/C'),$$

其中 $C'\subseteq B\subseteq G$. 我们断言 $G=A\oplus B$. 显然 $G=A+C'+B=A+B$（因为 $C'\subseteq B$），而 $A\cap B\subseteq A\cap((A+C')\cap B)=A\cap C'=\{0\}$. ■

260

定理 5.21（基定理） 每个有限阿贝尔群都是循环群的直和.

证明 对 $|G|\geqslant 1$ 用归纳法证明. 基础步显然为真. 为证明归纳步，设 p 是 $|G|$ 的素因数. 现在 $G=G_p\oplus H$，其中 $p\nmid |H|$（或者调用准素分解，或者对这种特殊情形重新证明）. 由归纳假设，H 是循环群的直和. 如果 G_p 是循环群，证明已经完成. 否则，运用引理 5.20 把 G_p 写作 $G_p=A\oplus B$，其中 A 是循环群. 由归纳假设，B 是循环群的直和，定理得证. ■

基定理的另一个短证明属于 R. Rado，*Journal London Mathematical Society* 26（1951），75～76 页和 160 页. 我们仅概要地证明.

设 G 是加法阿贝尔群，x_1，…，x_n 是 G 的元素. 作 $1\times n$ 矩阵 X，它的第 j 个元素是 x_j. 如果 U 是元素在$\mathbb{Z}$中的 $n\times n$ 矩阵，则 XU 是元素在 G 中的另一个 $1\times n$ 矩阵，这是因为它的元素是 $x_1,\cdots,x_n$的$\mathbb{Z}$-线性组合. 容易验证结合律：如果 U 和 V 是元素在$\mathbb{Z}$中的 $n\times n$ 矩阵，则 $X(UV)=(XU)V$. 此外，XU 生成的子群和 X 生成的子群之间有明显的关系，就是 $\langle XU\rangle\subseteq\langle X\rangle$.

引理 A 设 G 是加法阿贝尔群，x_1，…，x_n 是 G 的元素，X 是 $1\times n$ 矩阵，它的第 j 个元素是 x_j，并设 U 是元素在$\mathbb{Z}$中的 $n\times n$ 矩阵. 如果 $\det(U)=1$，则 $\langle XU\rangle=\langle X\rangle$.

定义 元素在 PID R 中的 $n\times 1$ 矩阵 $[a_1,\cdots,a_n]$ 称为**幺模列**，如果 $\gcd(a_1,\cdots,a_n)=1$.

引理 B 如果 R 是 PID，则每个幺模列 $[a_1,\cdots,a_n]$ 都是 R 上的某个满足 $\det(U)=1$ 的 $n\times n$ 矩阵 U 的第一列.

证明概要 对 $n\geqslant 2$ 用归纳法证明. 如果 $n=2$，则 R 中存在元素 s 和 t 使得 $ta_1+sa_2=1$ 且 $U=\begin{bmatrix}a_1 & -s\\ a_2 & t\end{bmatrix}$ 是行列式为 1 的矩阵. 关于归纳步，先令 $d=\gcd(a_1,\cdots,a_{n-1})$，并对 $i\leqslant n-1$ 定义 $b_i=a_i/d$. 因 $[b_1,\cdots,b_{n-1}]$ 是幺模列，归纳假设说它是行列式为 1 的 $(n-1)\times(n-1)$ 矩阵 U' 的第一列. 现在因 $[a_1,\cdots,a_n]$ 是幺模列，所以 $(a_n,d)=1$，从而存在 $s,t\in R$ 使得 $td+sa_n=1$. 可用这些数据巧妙地修改 U'，然后论证它形成一个 $n\times n$ 幺模矩阵，它的第一列是$[a_1,\cdots,a_n]$. ■

定理 （i）如果阿贝尔群 $G=\langle x_1,\cdots,x_n\rangle$ 且$[a_1,\cdots,a_n]$是幺模列，则存在 G 的 n 个生成元的集合，其中一个元素是 $a_1x_1+\cdots+a_nx_n$.

（ii）如果 $G=\langle x_1,\cdots,x_n\rangle$ 是有限阿贝尔群，则 G 是循环群的直和.

证明 （i）由引理 B，存在 $\det(U)=1$ 的 $n\times n$ 矩阵 U，它的第一列是 $[a_1,\cdots,a_n]$. 因 $\det(U)=1$，应用引理 A 表明 XU 的元素生成G，XU 的第一个元素是 $a_1x_1+\cdots+a_nx_n$.

261

（ii）设 n 是 G 的任意生成集的最小基数，并称这种生成集为极小生成集. 对极小生成集中的元素个数 n 用归纳法证明. 如果 $n=1$，则 G 是循环群，证明已经完成. 在极小生成集中的一切元素中取一个阶最小的，比如元素 x，阶为 k（从而没有一个极小生成集包含阶小于 k 的元素）. 选取包含 x 的极小生成集 $\{x_1,\cdots,x_{n-1},x\}$，并定义 $x_n=x$. 现在，由 n 的极小性，$H=\langle x_1,\cdots,x_{n-1}\rangle$ 是 G 的真子群. 又由归纳假设，H 是循环群的直和. 所以只需证明 $H\cap\langle x_n\rangle=\{0\}$，因为由此即可得到所要的 $G=H+\langle x_n\rangle=H\oplus\langle x_n\rangle$. 相反，如果 $\langle x_n\rangle\cap H\neq\{0\}$，则存在整数 $a_1,\cdots,a_n$ 使得 $a_nx_n\neq 0$ 且 $a_nx_n=\sum_{i=1}^{n-1}a_ix_i$（当然，可以假定 $0<a_n<k$）. 令 $d=\gcd(a_1,\cdots,a_n)$. 现在 $[a_1/d,\cdots,a_n/d]$ 是幺模列，根据（i），元素 $g=-(a_n/d)x_n+\sum_{i=1}^{n-1}(a_i/d)x_i$ 是 G 的极小生成集的一员. 但 $dg=0$，从而 g 的阶是 d 的因数，因此 g 是阶小于 k 的极小生成集的元素，这就产生矛盾. 所以 $\langle x_n\rangle\cap H=\{0\}$，从而 G 是循环群的直和. ■

5.1.3 基本定理

什么时候两个有限阿贝尔群 G 和 G' 同构? 由基定理，这种群是循环群的直和，因此我们的第一个猜想是 $G\cong G'$，如果它们拥有的每种类型的循环直和项的个数相等. 但这个希望被定理 2.81 破灭，该定理说，如果 m 和 n 互素，则 $\mathbb{I}_{mn}\cong\mathbb{I}_m\times\mathbb{I}_n$，例如，$\mathbb{I}_6\cong\mathbb{I}_2\times\mathbb{I}_3$. 于是我们退一步，尝试计算准素循环直和项. 但是该怎样做? 和算术基本定理中一样，我们必须要问这里是否存在某种唯一分解定理.

在开始下一引理之前，回忆已经定义的

$$d(G)=\dim(G/pG).$$

特别地，$d(pG)=\dim(pG/p^2G)$，更一般地，

$$d(p^nG)=\dim(p^nG/p^{n+1}G).$$

引理 5.22 设 G 是有限 p-准素阿贝尔群，其中 p 是素数，并设 $G=\sum_j C_j$，其中每个 C_j 是循环群. 如果 $b_n\geqslant 0$ 是阶为 p^n 的直和项 C_j 的个数，则存在某个 $t\geqslant 1$ 使得

$$d(p^nG)=b_{n+1}+b_{n+2}+\cdots+b_t.$$

证明 设 B_n 是阶为 p^n 的一切 C_j 的直和，如果有的话. 于是对某个 t 有

$$G=B_1\oplus B_2\oplus\cdots\oplus B_t.$$

现在因为对一切 $j\leqslant n$，$p^nB_j=\{0\}$，所以

$$p^nG=p^nB_{n+1}\oplus\cdots\oplus p^nB_t.$$

262

同样，

$$p^{n+1}G=p^{n+1}B_{n+2}\oplus\cdots\oplus p^{n+1}B_t.$$

现在命题 5.7 表明 $p^nG/p^{n+1}G$ 同构于

$$[p^nB_{n+1}/p^{n+1}B_{n+1}]\oplus[p^nB_{n+2}/p^{n+1}B_{n+2}]\oplus\cdots\oplus[p^nB_t/p^{n+1}B_t].$$

习题 5.7 给出对一切 $n<m$，$d(p^nB_m/p^{n+1}B_m)=\dim(p^nB_m)=b_m$. 因 d 在直和上可加，因而有

$$d(p^nG)=b_{n+1}+b_{n+2}+\cdots+b_t.$$ ■

现在数 b_n 可以用 G 来描述.

定义 设 G 是有限 p-准素阿贝尔群，其中 p 是素数. 对 $n\geqslant 0$，定义

$$U_p(n,G) = d(p^nG) - d(p^{n+1}G).$$

引理5.22表明

$$d(p^nG) = b_{n+1} + \cdots + b_t$$

和

$$d(p^{n+1}G) = b_{n+2} + \cdots + b_t,$$

从而 $U_p(n,G) = b_{n+1}$.

定理5.23 如果 p 是素数，则任意两种有限 p-准素阿贝尔群 G 的循环群直和分解拥有的每一种类型的循环直和项的个数相等. 更精确地说，对每个 $n \geqslant 0$，阶为 p^{n+1} 的循环直和项的个数是 $U_p(n,G)$.

证明 由基定理，存在循环子群 C_i 使得 $G = \sum_i C_i$. 引理表明，对每个 $n \geqslant 0$，阶为 p^{n+1} 的 C_i 的个数是 $U_p(n,G)$，这个数的定义未曾提及 G 的循环群直和分解. 于是，如果 $G = \sum_j D_j$ 是 G 的另一种分解，其中 D_j 是循环群，则阶为 p^{n+1} 的 D_i 的个数正如所要证明的，也是 $U_p(n,G)$. ■

系5.24 如果 G 和 G' 是有限 p-准素阿贝尔群，则 $G \cong G'$ 当且仅当对一切 $n \geqslant 0$，$U_p(n,G) = U_p(n,G')$.

证明 如果 $\varphi: G \to G'$ 是同构，则对一切 $n \geqslant 0$，$\varphi(p^nG) = p^nG'$，从而对一切 $n \geqslant 0$，φ 由 $p^ng + p^{n+1}G \mapsto p^n\varphi(g) + p^{n+1}G'$ 导出 $\mathbb{F}_p$-向量空间的同构 $p^nG/p^{n+1}G \cong p^nG'/p^{n+1}G'$，于是它们的维数相等，即 $U_p(n,G) = U_p(n,G')$.

反之，假定对一切 $n \geqslant 0$，$U_p(n,G) = U_p(n,G')$. 如果 $G = \sum_i C_i$ 和 $G' = \sum_j C'_j$，其中 C_i 和 C'_j 是循环群，则引理5.22表明每种类型直和项的个数相同，因此容易构造同构 $G \to G'$. ■

263

定义 如果 G 是 p-准素阿贝尔群，则它的**初等因子**是指下列序列中的数，这个序列有 $U_p(0,G)$ 个 p，$U_p(1,G)$ 个 p^2，…，$U_p(t-1,G)$ 个 p^t，其中 p^t 是 G 的循环直和项的最大阶.

如果 G 是有限阿贝尔群，则它的**初等因子**是它的所有准素分量的初等因子.

定理5.25（有限阿贝尔群的基本定理） 两个有限阿贝尔群 G 和 G' 同构当且仅当它们有相同的初等因子，即在 G 和 G' 的任意两种准素循环群直和分解中，每一阶的直和项的个数相同.

证明 由准素分解定理5.13(ii)，$G \cong G'$ 当且仅当对每个素数 p，它们的准素分量同构：$G_p \cong G'_p$. 现在由系5.24可得结论. ■

例5.26 72阶阿贝尔群有多少个？现在 $72 = 2^3 3^2$，因此任一72阶阿贝尔群都是8阶和9阶群的直和. 有3个8阶群，用初等因子来描述是

$$(2,2,2),(2,4) \quad 和 \quad (8);$$

有两个9阶群，用初等因子描述是

$$(3,3) \quad 和 \quad (9).$$

所以如果不计同构，有6个72阶阿贝尔群. ■

下面是有限阿贝尔群的第二种类型的循环群直和分解，它不提及准素群.

命题5.27 每个有限阿贝尔群 G 都是循环群的直和

$$G = S(c_1) \oplus S(c_2) \oplus \cdots \oplus S(c_t),$$

其中 $t \geqslant 1$，$S(c_i)$ 是 c_i 阶循环群，且

$$c_1 \mid c_2 \mid \cdots \mid c_t.$$

证明 设 p_1，…，p_n 是 $|G|$ 的素因数. 由基定理，对每个 p_i 有

$$G_{p_i} = S(p_i^{e_{i1}}) \oplus S(p_i^{e_{i2}}) \oplus \cdots \oplus S(p_i^{e_{it}}).$$

可以假定 $0 \leqslant e_{i1} \leqslant e_{i2} \leqslant \cdots \leqslant e_{it}$；此外，我们允许出现"虚假"指数 $e_{ij}=0$，从而对一切 i，最后的指标都可以用 t. 定义

$$c_j = p_1^{e_{1j}} p_2^{e_{2j}} \cdots p_n^{e_{nj}}.$$

显然 $c_1 \mid c_2 \mid \cdots \mid c_t$. 最后，定理 2.81 表明对每个 j，

$$S(p_1^{e_{1j}}) \oplus S(p_2^{e_{2j}}) \oplus \cdots \oplus S(p_n^{e_{nj}}) \cong S(c_j). \qquad ■$$

定义 如果 G 是阿贝尔群，则它的**指数**是指满足 $mG=\{0\}$ 的最小正整数 m.

系 5.28 如果 G 是有限阿贝尔群，$G = S(c_1) \oplus S(c_2) \oplus \cdots \oplus S(c_t)$，$S(c_i)$ 是 c_i 阶循环群，且 $c_1 \mid c_2 \mid \cdots \mid c_t$，则 c_t 是 G 的指数.

证明 因对一切 i，$c_i \mid c_t$，所以对一切 i 有 $c_t S(c_i)=0$，从而 $c_t G=\{0\}$. 另一方面，不存在满足 $1 \leqslant e < c_t$ 的数 e 使得 $eS(c_t)=\{0\}$，从而 c_t 是使 G 消失的最小的正整数. ■

系 5.29 每个非循环有限阿贝尔群 G 都有一个子群同构于 $\mathbb{I}_c \oplus \mathbb{I}_c$，其中 c 是某个 >1 的数.

证明 因 G 不是循环群，由命题 5.27，$G=\mathbb{I}_{c_1} \oplus \mathbb{I}_{c_2} \oplus \cdots \oplus \mathbb{I}_{c_t}$，其中 $t \geqslant 2$. 因 $c_1 \mid c_2$，所以循环群 $\mathbb{I}_{c_2}$ 包含一个子群同构于 $\mathbb{I}_{c_1}$，从而 G 有子群同构于 $\mathbb{I}_{c_1} \oplus \mathbb{I}_{c_1}$. ■

我们回到有限阿贝尔群的结构.

定义 如果 G 是有限阿贝尔群，又如果

$$G = S(c_1) \oplus S(c_2) \oplus \cdots \oplus S(c_t),$$

其中 $t \geqslant 1$，$S(c_j)$ 是 $c_j>1$ 阶循环群，且 $c_1 \mid c_2 \mid \cdots \mid c_t$，则称 c_1，c_2，…，c_t 为 G 的**不变因子**.

系 5.30 如果 G 是具有不变因子 $c_1,\cdots,c_t$ 和初等因子 $\{p_i^{e_{ij}}\}$ 的有限阿贝尔群，则 $|G| = \prod_{j=1}^{t} c_j = \prod_{ij} p_i^{e_{ij}}$，且它的指数是 c_t.

证明 我们有

$$G \cong \mathbb{Z}/(c_1) \oplus \cdots \oplus \mathbb{Z}/(c_t)$$
$$\cong \mathbb{I}_{c_1} \oplus \cdots \oplus \mathbb{I}_{c_t}.$$

因为一个直和的基础集合是笛卡儿积，我们有 $|G| = \prod_{j=1}^{t} c_j$ 和 $|G| = \prod_{ij} p_i^{e_{ij}}$. 在系 5.28 中证明了 c_t 是指数. ■

例 5.31 在例 5.26 中，我们展示了 72 阶阿贝尔群的初等因子，这里是它们的不变因子.

初等因子 ↔ 不变因子

(2,2,2,3,3) = (2,2,2,1,3,3) ↔ 2 | 6 | 6

(2,4,3,3) ↔ 6 | 12

(8,3,3) = (1,8,3,3) ↔ 3 | 24

(2,2,2,9) = (2,2,2,1,1,9) ↔ 2 | 2 | 18

(2,4,9) = (2,4,1,9) ↔ 2 | 36

(8,9) ↔ 72 ■

定理 5.32（不变因子） 两个有限阿贝尔群同构当且仅当它们有相同的不变因子.

证明 给定 G 的初等因子，如同命题 5.27 的证明一样，可以构造不变因子：

$$c_j = p_1^{e_{1j}} p_2^{e_{2j}} \cdots p_n^{e_{nj}},$$

其中不等于 $p_i^0=1$ 的那些因子 $p_i^{e_{i1}}, p_i^{e_{i2}}, \cdots$ 是 G 的 p_i-准素分量的初等因子. 因为不变因子是用初等因子来定义的，所以不变因子仅依赖于 G.

为证明同构，由基本定理，只需证明初等因子可以由不变因子计算出来. 因 $c_j = p_1^{e_{1j}} p_2^{e_{2j}} \cdots p_n^{e_{nj}}$，算术基本定理表明 c_j 确定了所有那些不等于 1 的素数幂 $p_i^{e_{ij}}$，即不变因子 c_j 确定初等因子. ■

在例 5.31 中，我们用初等因子计算不变因子，现在用不变因子来计算初等因子.

不变因子 ↔ 初等因子

$$2 \mid 6 \mid 6 = 2 \mid 2 \cdot 3 \mid 2 \cdot 3 \leftrightarrow (2,2,2,3,3)$$
$$6 \mid 12 = 2 \cdot 3 \mid 2^2 \cdot 3 \leftrightarrow (2,4,3,3)$$
$$3 \mid 24 = 3 \mid 2^3 \cdot 3 \leftrightarrow (8,3,3)$$
$$2 \mid 2 \mid 18 = 2 \mid 2 \mid 2 \cdot 3^2 \leftrightarrow (2,2,2,9)$$
$$2 \mid 36 = 2 \mid 2^2 \cdot 3^2 \leftrightarrow (2,4,9)$$
$$72 = 2^3 \cdot 3^2 \leftrightarrow (8,9).$$

在第 9 章中将把本节的结果从有限阿贝尔群推广到有限生成阿贝尔群. 阿贝尔群 G 称为有限生成的，如果存在有限个元素 $a_1, \cdots, a_n \in G$ 使得每个 $x \in G$ 都是它们的线性组合：$x = \sum_i m_i a_i$，其中对一切 i，$m_i \in \mathbb{Z}$. 基定理推广为：每个有限生成阿贝尔群 G 都是循环群的直和，这些循环群是有限准素群或无限循环群. 基本定理推广为：给定 G 的两种循环群直和分解（如在基定理中那样），在这两种分解中，同一类型的循环群直和项的个数相同. 基定理对非有限生成的阿贝尔群不再成立，例如有理数的加法群 $\mathbb{Q}$ 不是循环群的直和.

266

习题

5.1 (i) 设 G 是任意群（可以是非阿贝尔群），且设 S 和 T 是 G 的正规子群. 证明：如果 $S \cap T = \{1\}$，则对一切 $s \in S$ 和 $t \in T$，$st = ts$.

提示：证明 $sts^{-1}t^{-1} \in S \cap T$.

(ii) 证明：如果在命题 5.4 中假定一切子群 S_i 都是正规子群，则该命题对非阿贝尔群 G 成立：

5.2 设 G 是阿贝尔群，不必是准素的. 定义子群 $S \subseteq G$ 为**纯子群**，如果对一切 $m \in \mathbb{Z}$，

$$S \cap mG = mS.$$

证明：如果 G 是 p-准素阿贝尔群，则子群 $S \subseteq G$ 是刚才定义的纯子群当且仅当对一切 $n \geq 0$，$S \cap p^n G = p^n S$（课文中的定义）.

5.3 设 G 是阿贝尔群，它可以是无限的.

(i) 证明 G 的每个直和项 S 都是纯子群.

定义 G 的**挠**[⊖]**子群** tG 为

$$tG = \{a \in G : a \text{ 的阶有限}\}.$$

(ii) 证明 tG 是 G 的纯子群. [存在阿贝尔群 G，它的挠子群 tG 不是直和项（见习题9.1(iii)）. 因此纯子群未必是直和项.]

(iii) 证明 G/tG 是阿贝尔群，其中每个非零元素的阶都是无限的.

⊖ 该术语来自代数拓扑. 对每个空间 X，设计了一个阿贝尔群的序列，称为同调群，如果 X 是“扭曲”的，则这些群中有某些群包含有限阶元素.

5.4 设 p 是素数且 q 与 p 互素. 证明：如果 G 是 p-群且 $g\in G$，则存在 $x\in G$ 使得 $qx=g$.

5.5 设 $G=\langle a\rangle$是 m 阶有限循环群. 证明 G/nG 是 d 阶循环群，其中 $d=(m,n)$.

5.6 对于 m 阶循环群 $G=\langle a\rangle$和正整数 n，定义

$$G[n]=\{g\in G : g^n=1\}.$$

证明 $G[n]=\langle a^{m/d}\rangle$，其中 $d=(m,n)$. 由此推出 $G[n]\cong \mathbb{I}_d$.

5.7 证明：如果 $B=B_m=\langle x_1\rangle\oplus\cdots\oplus\langle x_{b_m}\rangle$是 b_m 个 p^m 阶循环群的直和，且 $n<m$，则陪集 $p^nx_i+p^{n+1}B(1\leqslant i\leqslant b_m)$是 $p^nB/p^{n+1}B$ 的基. 由此推出当 $n<m$ 时，$d(p^nB_m)=b_m$. [回忆如果 G 是有限阿贝尔群，则 G/pG是$\mathbb{F}_p$ 上的向量空间且 $d(G)=\dim(G/pG)$.]

267

5.8 (i) 如果 G 是有限 p-准素阿贝尔群，其中 p 是素数，且 $x\in G$ 有最大阶，证明$\langle x\rangle$是 G 的直和项.

(ii) 证明：如果 G 是有限阿贝尔群且 $x\in G$ 有极大阶（即 G 中没有阶更大的元素），则$\langle x\rangle$是 G 的直和项.

5.9 证明有限阿贝尔群的子群是直和项当且仅当它是纯子群.

提示：修改定理 5.18，即基定理的证明.

5.10 (i) 如果 G 和 H 都是有限阿贝尔群，证明对一切素数 p 和一切 $n\geqslant 0$，

$$U_p(n,G\oplus H)=U_p(n,G)+U_p(n,H).$$

(ii) 如果 A，B，C 都是有限阿贝尔群，证明 $A\oplus B\cong A\oplus C$ 蕴涵 $B\cong C$.

(iii) 如果 A，B 都是有限阿贝尔群，证明 $A\oplus A\cong B\oplus B$ 蕴涵 $A\cong B$.

5.11 如果 n 是正整数，则 n 的一个**划分**是指正整数序列 $i_1\leqslant i_2\leqslant\cdots\leqslant i_r$ 满足 $i_1+i_2+\cdots+i_r=n$. 如果 p 是素数，证明 p^n 阶不同构的阿贝尔群的个数等于 n 的划分的个数.

5.12 证明：如果不计同构，则恰好存在 14 个 288 阶阿贝尔群.

5.13 运用有限阿贝尔群的基本定理到 $G=\mathbb{I}_n$，证明算术基本定理中断言的唯一性.

5.14 (i) 如果 G 是有限阿贝尔群，定义

$$v_k(G)=G\text{ 中 }k\text{ 阶元素的个数}.$$

证明两个有限阿贝尔群 G 和 G'同构当且仅当对一切整数 k，$v_k(G)=v_k(G')$.

提示：如果 B 是一个 p^n 阶循环群的 k 个复制的直和，则 B 中有多少个 p^n 阶元素？

(ii) 举出两个不同构的群 G 和 G'的例子，它们不必是阿贝尔有限群，对于一切整数 k 有 $v_k(G)=v_k(G')$.

提示：取 G 为 p^3 阶群.

5.15 证明加法群$\mathbb{Q}$ 不是直和：$\mathbb{Q}\ncong A\oplus B$，其中 A，B 是非零子群.

提示：如果 a，$b\in\mathbb{Q}$ 非零，则存在 $c\in\mathbb{Q}$ 使得 $a,b\in\langle c\rangle$.

5.16 设 $G=B_1\oplus B_2\oplus\cdots\oplus B_t$，其中 B_i 是子群.

(i) 证明 $G[p]=B_1[p]\oplus B_2[p]\oplus\cdots\oplus B_t[p]$.

(ii) 证明对一切 $n\geqslant 0$，

$$\begin{aligned}p^nG\cap G[p]&=(p^nG\cap B_1[p])\oplus(p^nG\cap B_2[p])\oplus\cdots\oplus(p^nG\cap B_t[p])\\&=(p^nB_1\cap B_1[p])\oplus(p^nB_2\cap B_2[p])\oplus\cdots\oplus(p^nB_t\cap B_t[p]).\end{aligned}$$

(iii) 如果 G 是 p-准素阿贝尔群，证明对一切 $n\geqslant 0$，

$$U_p(n,G)=\dim\left(\frac{p^nG\cap G[p]}{p^{n+1}G\cap G[p]}\right).$$

268

5.2 西罗定理

我们回到非阿贝尔群，从而恢复乘法记号. 对于有限非阿贝尔群，西罗定理类似于有限阿贝尔群的准素分量.

回忆群 $G \neq \{1\}$ 称为单群，如果除了$\{1\}$和它自身之外没有其他正规子群．在命题 2.107 中，我们知道阿贝尔单群恰是阶为素数 p 的循环群I_p，而在定理 2.112 中，又知道对 $n \geqslant 5$，A_n 是非阿贝尔单群．事实上，A_5 是阶最小的非阿贝尔单群．如何证明阶小于 $60 = |A_5|$ 的非阿贝尔群 G 不是单群？习题 2.98 说明：如果 G 是群，阶为 $|G| = mp$，其中 p 是素数且 $1 < m < p$，则 G 不是单群．该习题表明许多小于 60 的数不是单群的阶．抛开一切素数幂之后（p-群不会是非阿贝尔单群），剩下可能的数只有

$$12,18,24,30,36,40,45,48,50,54,56.$$

该习题的解运用了柯西定理，柯西定理说 G 有 p 阶子群．我们将看到如果 G 有 p^e 阶子群而不是 p 阶子群，则可以推广习题 2.98，且可以缩短候选者的表．对于 G 的不同于循环子群的真子群我们知道些什么？群 G 的中心 $Z(G)$ 是可能的候选者，但这个子群可能不是真子群，也可能是平凡子群：如果 G 是阿贝尔群，则 $Z(G) = G$；如果 $G = S_3$，则 $Z(G) = \{1\}$．因此 $Z(G)$ 不能用来推广该习题．

1870 年出版的 C. Jordan 所著的《Traité des Substitutions et des Équations Algébriques》是关于群论的第一本书（一多半讲的是伽罗瓦理论，因而称为方程论）．几乎同时，发现了三个基本定理，但要在若尔当的书中发表已经为时太晚．1868 年，E. Schering 证明了基定理：每个有限阿贝尔群都是阶为素数幂的循环群的直积．1870 年，克罗内克在不知道 Schering 的证明的情况下也证明了该结果．1878 年，费罗贝尼乌斯（F. G. Frobenius）和施蒂克贝格（L. Stickelberger）证明了有限阿贝尔群的基本定理．1872 年，西罗证明，对每个有限群 G 和每个素数 p，如果 p^e 是整除 $|G|$ 的 p 的最高幂，则 G 有一个 p^e 阶子群，今日叫做*西罗子群*，我们将用这个子群来推广习题 2.98．如果采用下面的定义将使证明西罗定理的策划进行得十分顺利．

定义　*设 p 是素数．有限群 G 的***西罗 p-子群***是极大 p-子群 P．*

极大性的意思是：如果 Q 是 G 的 p-子群且 $P \leqslant Q$，则 $P = Q$．

根据拉格朗日定理，如果 p^e 是整除 $|G|$ 的 p 的最高幂，则一个 p^e 阶子群（要是存在的话）是 G 的极大 p-子群．现在的定义的一个好处是极大 p-子群恒存在：确实，我们可以证明，如果 S 是 G 的任一 p-子群（有可能 $S = \{1\}$），则存在西罗 p-子群 P 包含 S．如果不存在 p-子群严格地包含 S，则 S 自己就是一个西罗 p-子群．否则存在 p-子群 P_1 使得 $S < P_1$．如果 P_1 是极大的，则它就是西罗 p-子群，证明已经完成．否则存在某个 p-子群 P_2 使得 $P_1 < P_2$．产生一个比一个大的 p-子群 P_i 的这个过程经有限步后必终止，因为对一切 i，$|P_i| \leqslant |G|$，因此最大的 P_i 必是西罗 p-子群．

269

回忆子群 $H \leqslant G$ 的一个共轭是 G 的一个形如

$$aHa^{-1} = \{aha^{-1} : h \in H\}$$

的子群，其中 $a \in G$．G 中 H 的*正规化子*是子群

$$N_G(H) = \{a \in G : aHa^{-1} = H\},$$

命题 2.101 表明如果 H 是有限群 G 的子群，则 G 中 H 的共轭的个数是 $[G : N_G(H)]$．

显然 $H \lhd N_G(H)$，从而商群 $N_G(H)/H$ 有定义．

引理 5.33　*设 P 是有限群 G 的一个西罗 p-子群．*

（i）P 的每个共轭也是 G 的西罗 p-子群．

（ii）$|N_G(P)/P|$ 与 p 互素．

（iii）如果 $a \in G$ 的阶为 p 的某个幂且 $aPa^{-1} = P$，则 $a \in P$．

证明　（i）如果 $a \in G$，则 aPa^{-1} 是 G 的 p-子群．如果它不是极大 p-子群，则存在 p-子群

Q 使得 $aPa^{-1}<Q$. 因此 $P<a^{-1}Qa$，与 p 的极大性矛盾.

（ⅱ）如果 p 整除 $|N_G(P)/P|$，则柯西定理表明 $N_G(P)/P$ 包含 p 阶元素 aP，因此 $N_G(P)/P$ 包含 p 阶子群 $S^*=\langle aP\rangle$. 由对应定理（定理 2.76），存在满足 $P\leqslant S\leqslant N_G(P)$ 的子群 S 使得 $S/P\cong S^*$. 而 S 是 $N_G(P)\leqslant G$ 的 p-子群（根据习题 2.75），它严格地大于 P，与 P 的极大性矛盾. 由此可知 P 不整除 $|N_G(P)/P|$.

（ⅲ）由正规化子的定义，元素 a 在 $N_G(P)$ 中. 如果 $a\notin P$，则陪集 aP 是 $N_G(P)/P$ 的非平凡元素，其阶为 p 的某个幂；依据（ⅱ），这与拉格朗日定理矛盾. ■

因为西罗 p-子群的每个共轭也是西罗 p-子群，所以令 G 用共轭作用在西罗 p-子群上是合理的.

定理 5.34（西罗） 设 G 是有限群，阶为 $p_1^{e_1}\cdots p_t^{e_t}$，并设 P 是 G 的西罗 p-子群，其中 p 是某个素数 $p=p_j$.

（ⅰ）每个西罗 p-子群都与 P 共轭.

（ⅱ）如果存在 r_j 个西罗 p_j-子群，则 r_j 是 $|G|/p_j^{e_j}$ 的因数，且

$$r_j\equiv 1 \bmod p_j.$$

证明 设 $X=\{P_1,\cdots,P_{r_j}\}$ 是 P 的一切共轭的集合，其中记 P 为 P_1. 如果 Q 是 G 的任意一个西罗 p-子群，则 Q 用共轭作用在 X 上：如果 $a\in Q$，则它发送

$$P_i=g_iPg_i^{-1}\mapsto a(g_iPg_i^{-1})a^{-1}=(ag_i)P(ag_i)^{-1}\in X.$$

根据系 2.99，任一轨道中的元素个数是 $|Q|$ 的因数，即每个轨道的大小是 p 的某个幂（因为 Q 是 p-群）. 如果有一个轨道的大小为 1，则存在某个 P_i 使得对一切 $a\in Q$，$aP_ia^{-1}=P_i$. 根据引理 5.33，对一切 $a\in Q$ 有 $a\in P_i$；即 $Q\leqslant P_i$. 而 Q 是一个西罗 p-子群，它是 G 的极大 p-子群，从而 $Q=P_i$. 特别地，如果 $Q=P_1$，则只有一个大小为 1 的轨道，它就是 $\{P_1\}$，其他一切轨道的大小都是 p 的真正的幂. 由此可知，$|X|=r_j\equiv 1 \bmod p$.

现在假设存在某个西罗 p-子群 Q，它不是 P 的共轭，即对任意 i，$Q\neq P_i$. 我们还是令 Q 作用在 X 上，如果有大小为 1 的轨道，比如 $\{P_k\}$. 和上一段一样，这蕴涵 $Q=P_k$，与我们现在的假设 $Q\notin X$ 相矛盾. 因此没有大小为 1 的轨道，这就是说每个轨道的大小都是 p 的真正的幂. 由此 $|X|=r_j$ 是 p 的倍数，即 $r_j\equiv 0 \bmod p$，与 $r_j\equiv 1 \bmod p$ 矛盾. 所以这样的 Q 不存在，从而一切西罗 p-子群都和 P 共轭.

最后，因一切西罗 p-子群都是共轭的，所以有 $r_j=[G:N_G(P)]$，从而 r_j 是 $|G|$ 的因数. 而 $r_j\equiv 1 \bmod p_j$ 蕴涵 $(r_j,p_j^{e_j})=1$，所以由欧几里得引理，$r_j\mid |G|/p_j^{e_j}$. ■

系 5.35 有限群 G 对某个素数 p 有唯一的西罗 p-子群 P，当且仅当 $P\lhd G$.

证明 假定 G 的西罗 p-子群 P 是唯一的. 对每个 $a\in G$，共轭 aPa^{-1} 也是西罗 p-子群. 由唯一性，对一切 $a\in G$，$aPa^{-1}=P$，从而 $P\lhd G$.

反之，假定 $P\lhd G$. 如果 Q 是任一西罗 p-子群，则对某个 $a\in G$ 有 $Q=aPa^{-1}$. 但由正规性，$aPa^{-1}=P$，所以 $Q=P$. ■

下面的结果给出西罗子群的阶.

定理 5.36（西罗） 如果 G 是 p^em 阶有限群，其中 p 是素数且 $p\nmid m$，则 G 的每个西罗 p-子群 P 的阶为 p^e.

证明 先证明 $p\nmid[G:P]$. 现在

270

[271]

$$[G:P]=[G:N_G(P)][N_G(P):P].$$

第一个因子 $[G:N_G(P)]=r$ 是 G 中 P 的共轭的个数，因为 $r\equiv 1 \bmod p$，所以 p 不整除 $[G:N_G(P)]$. 第二个因子 $[N_G(P):P]=|N_G(P)/P|$，根据引理 5.33，也不能被 p 整除. 所以，由欧几里得引理，p 不能整除 $[G:P]$.

现在有某个 $k\leqslant e$ 使得 $|P|=p^k$，从而

$$[G:P]=|G|/|P|=p^e m/p^k=p^{e-k}m.$$

因 p 不整除 $[G:P]$，必有 $k=e$；即 $|P|=p^e$. ■

例 5.37 (i) 设 $G=S_4$. 现在 $|S_4|=24=2^3 3$. 于是 S_4 的一个西罗 2-子群的阶为 8. 在练习 2.83 中我们已经看到，S_4 包含由正方形的对称组成的二面体群 D_8 的一个复制. 西罗定理说一切 8 阶子群都共轭（因此同构）于 D_8. 此外，西罗 2-子群的个数 r 是 24 的因数，对 mod 2 同余于 1；即 r 是 24 的奇因数. 因 $r\neq 1$（见习题 5.17），恰有 3 个西罗 2-子群.

(ii) 如果 G 是有限阿贝尔群，则一个西罗 p-子群正是它的 p-准素分量（因 G 是阿贝尔群，每个子群都是正规子群，从而对每个素数 p 存在唯一的西罗 p-子群）. ■

下面是后一个西罗定理的第二个证明，属于维兰特（H. Wielandt）.

定理 5.38 如果 G 是 $p^e m$ 阶有限群，其中 p 是素数且 $p\nmid m$，则 G 有 p^e 阶子群.

证明 设 X 是 G 的一切恰有 p^e 个元素的子集的族，则 $|X|=\binom{p^e m}{p^e}$. 根据习题 1.29，$p\nmid |X|$. 现在 G 作用在 X 上：对 $g\in G$ 和 $B\in X$，定义 gB 为

$$gB=\{gb: b\in B\}.$$

如果对每个 $B\in X$，p 整除 $|\mathcal{O}(B)|$，其中 $\mathcal{O}(B)$ 是 B 的轨道，则因为根据命题 2.97 X 是轨道的不相交并，所以 p 是 $|X|$ 的因数. 由于 $p\nmid |X|$，因此存在子集 B 满足 $|B|=p^e$ 且 $|\mathcal{O}(B)|$ 不能被 p 整除. 如果 G_B 是这个子集 B 的稳定化子，则定理 2.98 给出 $[G:G_B]=|\mathcal{O}(B)|$，从而 $|G|=|G_B|\cdot|\mathcal{O}(B)|$. 因 $p^e \mid\mid |G|$ 且 $p\nmid |\mathcal{O}(B)|$，反复运用欧几里得引理得 $p^e \mid\mid |G_B|$. 所以 $p^e\leqslant |G_B|$.

关于反过来的不等式，选取一个元素 $b\in B$ 并定义函数 $\tau: G_B\to B$ 为 $g\mapsto gb$. 注意，因为 $g\in G_B$，其中 G_B 是 B 的稳定化子，所以 $\tau(g)=gb\in gB=B$. 如果 $g,h\in G_B$ 且 $h\neq g$，则 $\tau(h)=hb\neq gb=\tau(g)$；即 τ 是单射. 由此可知 $|G_B|\leqslant |B|=p^e$，从而 G_B 是 G 的 p^e 阶子群. ■

[272]

命题 5.39 一切西罗子群都是正规子群的有限群 G 是它的西罗子群的直积.

证明 设 $|G|=p_1^{e_1}\cdots p_t^{e_t}$，并设 G_{p_i} 是 G 的西罗 p_i-子群. 我们运用习题 5.1，它是命题 5.4 在非阿贝尔群上的推广. 由一切西罗子群生成的子群 S 是 G，这是因为对一切 i，$p_i^{e_i} \mid\mid |S|$. 最后，如果 $x\in G_{p_i}\cap\langle\bigcup_{j\neq i}G_{p_j}\rangle$，则 $x=s_i\in G_{p_i}$，且 $x=\prod_{j\neq i}s_j$，其中 $s_j\in G_{p_j}$. 现在对某个 $n\geqslant 1$ 有 $x^{p_i^n}=1$. 另一方面，存在 p_j 的某个幂，比如 q_j，使得对一切 j，$s_j^{q_j}=1$. 根据习题 5.1，s_j 相互可交换，因此有 $1=x^q=(\prod_{j\neq i}s_j)^q$，其中 $q=\prod_{j\neq i}q_j$. 因 $(p_i^n,q)=1$，所以存在整数 u 和 v 使得 $1=up_i^n+vq$，从而 $x=x^1=x^{up_i^n}x^{vq}=1$. 所以 G 是它的西罗子群的直积. ■

我们现在推广习题 2.98 和它的解.

引理 5.40 不存在 $|G|=p^e m$ 阶的非阿贝尔单群 G，其中 p 是素数，$p\nmid m$ 且 $p^e\nmid(m-1)!$.

证明 我们断言：如果 p 是素数，则每个满足 $|G|>p$ 的 p-群 G 都不是单群. 定理 2.75 说中心 $Z(G)$ 是非平凡的. 但 $Z(G)\lhd G$，因此，如果 $Z(G)$ 是真子群，则 G 不是单群. 如果 $Z(G)=G$，

则 G 是阿贝尔群，命题 2.78 说除非 $|G|=p$，否则 G 不是单群.

假设这样的单群 G 存在. 由西罗定理，G 包含一个 p^e 阶子群 P，因而它的指数是 m. 因为非阿贝尔 p-群不会是单群，所以可以假定 $m>1$. 由定理 2.88，存在同态 $\varphi: G\to S_m$ 使得 $\ker\varphi\leqslant P$. 然而 G 是单群，它没有真正规子群，因此 $\ker\varphi=\{1\}$，从而 φ 是单射，即 $G\cong\varphi(G)\leqslant S_m$. 根据拉格朗日定理，$p^e m\mid m!$，从而 $p^e\mid(m-1)!$，与假设矛盾. ■

命题 5.41 不存在阶小于 60 的非阿贝尔单群.

证明 读者可以验证介于 2 和 59 之间的整数 n，它既不是素数幂也没有引理陈述中的形如 $n=p^e m$ 的因数分解，这样的 n 是 30,40 和 56. 根据引理只有这三个数可能是阶小于 60 的非阿贝尔单群的阶.

假定存在 30 阶单群 G. 令 P 是 G 的西罗 5-子群，从而 $|P|=5$. P 的共轭的个数 r_5 是 30 的因数且 $r_5\equiv 1\bmod 5$. 现在 $r_5\neq 1$，否则 $P\lhd G$，所以 $r_5=6$. 根据拉格朗日定理，这些群中任意两个的交是平凡群（西罗子群的交可能更复杂，见习题 5.18）. 每个群中有四个非幺元的元素，所以它们的并中有 $6\times 4=24$ 个非幺元的元素. 类似地，G 的西罗 3-子群的个数 r_3 是 10（因为 $r_3\neq 1$，所以 r_3 是 30 的因数且 $r_3\equiv 1\bmod 3$）. 每个这种群有两个非幺元的元素，从而，这些群的并中有 20 个非幺元的元素. 我们算出的元素个数已经超过了 G 中元素的个数，所以 G 不是单群. 273

设 G 是 40 阶群，并设 P 是 G 的西罗 5-子群. 如果 r 是 P 的共轭的个数，则 $r\mid 40$ 且 $r\equiv 1\bmod 5$. 这些条件迫使 $r=1$，从而 $P\lhd G$，所以不存在 40 阶单群.

最后，假定存在 56 阶单群 G. 如果 P 是 G 的西罗 7-子群，则 P 必有 $r_7=8$ 个共轭（因为 $r_7\mid 56$ 且 $r_7\equiv 1\bmod 7$）. 因为这些群是素数阶循环群，它们任一对的交是 $\{1\}$，所以在它们的并中有 48 个非幺元的元素，加上幺元，总共有 49 个 G 的元素. 现在一个西罗 2-子群 Q 的阶为 8，有 7 个非幺元的元素，总共已有 56 个元素. 但是还有第二个西罗 2-子群，否则 $Q\lhd G$，因此已经超过了我们的限额. 所以不存在 56 阶单群. ■

拉格朗日定理的"逆定理"不成立：如果 G 是 n 阶有限群且 $d\mid n$，则 G 可以没有 d 阶子群. 例如我们在命题 2.64 中证明交错群 A_4 是 12 阶群，它没有 6 阶子群.

命题 5.42 设 G 是有限群. 如果 p 是素数且 p^k 整除 $|G|$，则 G 有 p^k 阶子群.

证明 如果 $|G|=p^e m$，其中 $p\nmid m$，则 G 的一个西罗 p-子群的阶为 p^e. 因此，如果 p^k 整除 $|G|$，则 p^k 整除 $|P|$. 根据命题 2.106，P 有 p^k 阶子群，这样 G 有 p^k 阶子群. ■

我们已经知道哪些 p-群的例子？当然，p^n 阶循环群是 p-群，这些群的复制的直积也是 p-群. 根据基本定理，这些就是一切（有限）阿贝尔 p-群. 至今我们已知的非阿贝尔群的例子只有二面体群 D_{2n}（当 n 是 2 的幂时，它是 2-群）和阶为 8 的四元数群 $\mathbf{Q}$（当然，对每个 2-群 A，直积 $D_8\times A$ 和 $\mathbf{Q}\times A$ 也是非阿贝尔 2-群）. 下面是一些新例.

定义 域 k 上的**幺三角**矩阵是指对角线元素为 1 的上三角矩阵. 定义 $\mathrm{UT}(n,k)$ 为 k 上一切 $n\times n$ 幺三角矩阵的集合.

注 这个定义可以推广到 k 是任意交换环. 例如群 $\mathrm{UT}(n,\mathbb{Z})$ 就是一个有趣的群.

命题 5.43 如果 k 是域，则 $\mathrm{UT}(n,k)$ 是 $\mathrm{GL}(n,k)$ 的子群.

证明 单位矩阵 I 当然是幺三角矩阵，所以 $I\in\mathrm{UT}(n,k)$. 如果 $A\in\mathrm{UT}(n,k)$，则 $A=I+N$，其中 N 是严格上三角矩阵；即 N 是对角线元素为 0 的上三角矩阵. 注意严格上三角矩阵的和与积仍是严格上三角矩阵. 274

设 $e_1, \cdots, e_n$ 是 k^n 的标准基. 如果 N 是严格上三角矩阵，定义 $T: k^n \to k^n$ 为 $T(e_i) = Ne_i$，其中 e_i 看作列矩阵. 现在对一切 i，T 满足

$$T(e_1) = 0 \quad 和 \quad T(e_{i+1}) \in \langle e_1, \cdots, e_i \rangle.$$

对 i 用归纳法，易知

$$对一切\ j \leqslant i, T^i(e_j) = 0.$$

由此 $T^n = 0$ 并因此 $N^n = 0$. 于是，如果 $A \in \mathrm{UT}(n,k)$，则 $A = I + N$，其中 $N^n = 0$.

为证明 $\mathrm{UT}(n,k)$ 是 $\mathrm{GL}(n,k)$ 的子群，首先注意到 $(I+N)(I+M) = I + (N+M+NM)$ 是幺三角矩阵. 其次证明如果 A 是幺三角矩阵，则 A 是非奇异的且它的逆也是幺三角矩阵. 类似于幂级数展开式 $1/(1+x) = 1 - x + x^2 - x^3 + \cdots$，我们定义 $A = I + N$ 的逆为 $B = I - N + N^2 - N^3 + \cdots$（注意这个级数在 $n-1$ 项后终止，因为 $N^n = 0$），读者可验证 $BA = I = AB$，所以 $B = A^{-1}$. 此外，N 是严格上三角矩阵蕴涵 $-N + N^2 - N^3 + \cdots \pm N^{n-1}$ 也是严格上三角矩阵，从而 A^{-1} 是幺三角矩阵.（对于熟悉线性代数的读者可用另一种证法，我们知道 A 是非奇异的，因为它的行列式为 1，由 A 的伴随矩阵（余子式组成的矩阵）求 A^{-1} 的公式表明 A^{-1} 是幺三角矩阵.）因此 $\mathrm{UT}(n,k)$ 是 $\mathrm{GL}(n,k)$ 的子群. ■

命题 5.44 *设 $q = p^e$，其中 p 是素数. 对每个 $n \geqslant 2$, $\mathrm{UT}(n, \mathbb{F}_q)$ 是阶为 $q^{\binom{n}{2}} = q^{n(n-1)/2}$ 的 p-群.*

证明 一个 $n \times n$ 幺三角矩阵中严格位于对角线之上的元素个数是 $\binom{n}{2} = \frac{1}{2}n(n-1)$（从总共 n^2 个元素中抛开 n 个对角线上的元素，剩下 $n^2 - n$ 个元素的一半是对角线以上的元素）. 因这些元素的每一个都可以是 $\mathbb{F}_q$ 的任意元素，$\mathbb{F}_q$ 上恰存在 $q^{\binom{n}{2}}$ 个 $n \times n$ 幺三角矩阵，所以这是 $\mathrm{UT}(n, \mathbb{F}_q)$ 的阶. ■

回忆习题 2.26：如果 G 是群且对一切 $x \in G$，$x^2 = 1$，则 G 是阿贝尔群. 现在我们问：一个群 G 满足对一切 $x \in G, x^p = 1$，其中 p 是奇素数，该群是否也必是阿贝尔群.

命题 5.45 *如果 p 是奇素数，则存在 p^3 阶非阿贝尔群 G 满足对一切 $x \in G, x^p = 1$.*

证明 如果 $G = \mathrm{UT}(3, \mathbb{F}_p)$，则 $|G| = p^3$. 现在 G 是非阿贝尔群，例如矩阵

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad 和 \quad \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

275

不交换. 如果 $A \in G$，则 $A = I + N$，因 p 是奇素数，$p \geqslant 3$，从而 $N^p = 0$. 易知形如 $a_0 I + a_1 N + \cdots + a_m N^m$ 的一切矩阵的集合是一个交换环，其中 $a_i \in \mathbb{F}_p$，且这个交换环满足对一切 M，$pM = 0$. 而命题3.2(ⅵ)说在每个交换环中二项式定理成立；因为当 $1 < i < p$ 时，根据命题 1.12，$p \mid \binom{p}{i}$，因而有

$$A^p = (I + N)^p = I^p + N^p = I.$$ ■

定理 5.46 *令 $\mathbb{F}_q$ 表示有 q 个元素的有限域，则*

$$|\mathrm{GL}(n, \mathbb{F}_q)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}).$$

证明 设 V 是 $\mathbb{F}_q$ 上的 n 维向量空间. 我们先证明存在双射 $F: \mathrm{GL}(n, \mathbb{F}_q) \to \mathcal{B}$，其中 $\mathcal{B}$ 是 V 的一切基的集合. 选定 V 的一组基 $e_1, \cdots, e_n$. 如果 $T \in \mathrm{GL}(n, \mathbb{F}_q)$，定义

$$\Phi(T) = Te_1, \cdots, Te_n.$$

根据引理 3.103，因为 T 是非奇异的，它把基带到基，所以 $\Phi(T) \in \mathcal{B}$. 但 Φ 是双射，这是因为对于给出的一组基 $v_1, \cdots, v_n$，存在唯一的线性变换 S 使得对一切 i，$Se_i = v_i$（根据定理 3.92），而这个线性变换必定是非奇异的（根据引理 3.103）.

现在的问题是计算 V 的基 $v_1, \cdots, v_n$ 的个数. V 中有 q^n 个向量，因此 v_1 有 $q^n - 1$ 个候选者（零向量不是候选者），选好 v_1 之后我们知道 v_2 的候选者是那些不在 v_1 张成的子空间 $\langle v_1 \rangle$ 中的向量，于是 v_2 的候选者有 $q^n - q$ 个. 更一般地，已经选好线性无关表 $v_1, \cdots, v_i$ 之后，v_{i+1} 可以是不在 $\langle v_1, \cdots, v_i \rangle$ 中的任一向量，所以 v_{i+1} 的候选者有 $q^n - q^i$ 个. 对 n 用归纳法可得结论. ■

定理 5.47 *如果 p 是素数且 $q = p^m$，则幺三角矩阵群 $\mathrm{UT}(n, \mathbb{F}_q)$ 是 $\mathrm{GL}(n, \mathbb{F}_q)$ 的西罗 p-子群.*

证明 因 $q^n - q^i = q^i(q^{n-i} - 1)$，整除 $|\mathrm{GL}(n, \mathbb{F}_q)|$ 的 p 的最高幂是

$$qq^2q^3 \cdots q^{n-1} = q^{\binom{n}{2}}.$$

而 $|\mathrm{UT}(n, \mathbb{F}_q)| = q^{\binom{n}{2}}$，因此它必是西罗 p-子群. ■

系 5.48 *如果 p 是素数且 G 是有限 p-群，则 G 同构于幺三角矩阵群 $\mathrm{UT}(|G|, \mathbb{F}_p)$ 的一个子群.*

证明 先证明对每个 $m \geqslant 1$，对称群 S_m 可以嵌入 $\mathrm{GL}(m, k)$，其中 k 是域. 设 V 是 k 上的 m 维向量空间，且 $v_1, \cdots, v_m$ 是 V 的一组基. 定义函数 $\varphi: S_m \to \mathrm{GL}(V)$ 为 $\sigma \mapsto T_\sigma$，其中对一切 i，$T_\sigma: v_i \mapsto v_{\sigma(i)}$. 易知 φ 是单同态. 根据凯莱（Cayley）定理，G 可以嵌入 S_G，因此 G 可以嵌入 $\mathrm{GL}(m, \mathbb{F}_p)$，其中 $m = |G|$. 现在因为每个 p-子群在某个西罗 p-子群中，所以 G 包含在 $\mathrm{GL}(m, \mathbb{F}_p)$ 的某个西罗 p-子群 P 中. 因一切西罗 p-子群都共轭，因此存在 $a \in \mathrm{GL}(m, \mathbb{F}_p)$ 使得 $P = a(\mathrm{UT}(m, \mathbb{F}_p))a^{-1}$. 所以 [276]

$$G \cong a^{-1}Ga \leqslant a^{-1}Pa \leqslant \mathrm{UT}(m, \mathbb{F}_p).$$ ■

一个自然的问题是求对称群的西罗子群. 这是可以做到的，答案是用所谓的圈积来构造（见 Rotman 所著的《An Introduction to the Theory of Groups》，176 页）.

习题

5.17 S_4 有几个西罗 2-子群？

5.18 举出一个有限群 G 的例子，它有西罗 p-子群（p 是某个素数）P，Q 和 R 满足 $P \cap Q = \{1\}$ 及 $P \cap R \neq \{1\}$.

提示：考虑 $S_3 \times S_3$.

5.19 群 G 的子群 H 称为**特征子群**，如果对每个同构 $\varphi: G \to G, \varphi(H) \leqslant H$. 群 G 的子群 S 称为**全不变子群**，如果对每个同态 $\varphi: G \to G, \varphi(S) \leqslant S$.

(i) 证明每个全不变子群都是特征子群，且每个特征子群都是正规子群.

(ii) 证明换位子子群 G' 是群 G 的全不变子群，从而证明它是 G 的正规子群.

(iii) 举出一个群 G 的例子，它有不是特征子群的正规子群 H.

(iv) 证明群 G 的中心 $Z(G)$ 是特征子群（从而 $Z(G) \lhd G$），但它未必是全不变子群.

提示：令 $G = S_3 \times \mathbb{I}_2$.

(v) 证明：对每个群 G，如果 $H \lhd G$，则 $Z(H) \lhd G$.

5.20 如果 G 是阿贝尔群，证明对一切正整数 m，mG 和 $G[m]$ 是全不变子群.

5.21 **(费拉蒂尼命题)** 设 K 是有限群 G 的正规子群. 如果对某个素数 p, P 是 K 的西罗 p-子群, 证明

$$G = KN_G(P),$$

其中 $KN_G(P) = \{ab : a \in K\}$ 且 $b \in N_G(P)\}$.

提示: 如果 $g \in G$, 则 gPg^{-1} 是 K 的西罗 p-子群, 从而它是 P 在 K 中的共轭.

5.22 证明 $\mathrm{UT}(3,2) \cong D_8$, 由此推出 D_8 是 $\mathrm{GL}(3,2)$ 的西罗 2-子群.

提示: 可以用 8 阶非阿贝尔群只有 D_8 和 $\mathbf{Q}$ 的事实.

5.23 (i) 证明: 如果 d 是 24 的正因数, 则 S_4 有 d 阶子群.

277 (ii) 设 $d \neq 4$, 证明 S_4 的任两个 d 阶子群同构.

5.24 (i) 求 S_6 的西罗3-子群.

提示: $\{1,2,3,4,5,6\} = \{1,2,3\} \cup \{4,5,6\}$.

(ii) 证明 S_6 的西罗 2-子群同构于 $D_8 \times \mathbb{I}_2$.

提示: $\{1,2,3,4,5,6\} = \{1,2,3,4\} \cup \{5,6\}$.

5.25 设 Q 是有限群 G 的正规 p-子群. 证明对 G 的每个西罗 p-子群 P, $Q \leqslant P$.

提示: 用 G 的其他任一西罗 p-子群和 P 共轭的事实.

5.26 (i) 设 G 是有限群, P 是 G 的西罗 p-子群. 如果 $H \lhd G$, 证明 HP/H 是 G/H 的西罗 p-子群且 $H \cap P$ 是 H 的西罗 p-子群.

提示: 证明 $[G/H : HP/H][H : H \cap P]$ 与 p 互素.

(ii) 设 P 是有限群 G 的西罗 p-子群. 举出一个例子, 使得 H 是 G 的子群, 而 $H \cap P$ 不是 H 的西罗 p-子群.

提示: 选取 S_4 的子群 H 使得 $H \cong S_3$, 并求 S_4 的西罗 3-子群 P 使得 $H \cap P = \{1\}$.

5.27 证明 A_5 的一个西罗 2-子群恰有五个共轭.

5.28 证明没有 96 阶, 120 阶, 300 阶, 312 阶和 1 000 阶的单群.

提示: 其中有些是容易处理的.

5.29 设 G 是 90 阶群.

(i) 如果 G 的一个西罗 5-子群 P 不是正规子群, 证明它有六个共轭.

提示: 如果 P 有 18 个共轭, G 中就有 72 个 5 阶元素, 证明 G 的其他元素不止 18 个.

(ii) 证明 G 不是单群.

提示: 用习题2.95(ii)和习题2.96(ii).

5.30 证明没有 120 阶单群.

5.31 证明没有 150 阶单群.

5.32 如果 H 是有限群 G 的真子群, 证明 G 不是 H 的一切共轭的并; 即 $G \neq \bigcup_{x \in G} xHx^{-1}$.

5.3 若尔当-赫尔德定理

伽罗瓦引进群来研究 $k[x]$ 中的多项式, 其中 k 是特征 0 的域, 他发现这样的多项式运用根式可解当且仅当它的伽罗瓦群是可解群. 可解群就其自身来说也是群的一个重要的族, 我们现在进一步考察它.

回忆群 G 的正规列是 G 的子群的有限序列, $G = G_0, G_1, G_2, \cdots, G_n = \{1\}$, 满足

$$G = G_0 \geqslant G_1 \geqslant G_2 \geqslant \cdots \geqslant G_n = \{1\}$$

且对一切 i, $G_{i+1} \lhd G_i$. 这个序列的因子群是群 $G_0/G_1, G_1/G_2, \cdots, G_{n-1}/G_n$, 序列的长度是严格包含

的个数（等价地说，长度是非平凡因子群的个数），G 称为可解的，如果在它的正规列中，因子群都是素数阶循环群.

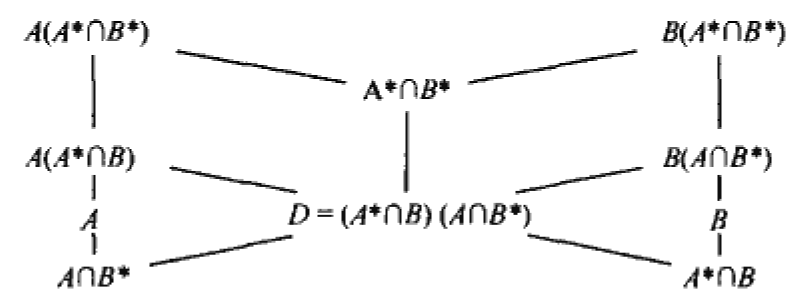
278

我们从推广第二同构定理的一个技术性的结果开始，因为要比较一个群的不同的正规列.

引理 5.49（扎森豪斯引理） 给定 G 的四个子群 $A \lhd A^*$ 和 $B \lhd B^*$，则 $A(A^* \cap B) \lhd A(A^* \cap B^*)$，$B(B^* \cap A) \lhd A(B^* \cap A^*)$，且存在同构

$$\frac{A(A^* \cap B^*)}{A(A^* \cap B)} \cong \frac{B(B^* \cap A^*)}{B(B^* \cap A)}.$$

注 扎森豪斯（Zassenhaus）引理有时因下面的图而称为蝴蝶引理. 我承认我从来就不喜欢这个图，它并不能使我联想起一只蝴蝶，而且它也不能帮助我理解或记忆证明.



引理中的同构在下列意义下对称：交换左端的符号 A，B 得到右端.

证明 我们断言 $(A \cap B^*) \lhd (A^* \cap B^*)$；即如果 $c \in A \cap B^*$，$x \in A^* \cap B^*$，则 $xcx^{-1} \in A \cap B^*$. 现在因 $c \in A$，$x \in A^*$ 且 $A \lhd A^*$，所以 $xcx^{-1} \in A$. 但因 $c, x \in B^*$，所以也有 $xcx^{-1} \in B^*$. 因此 $(A \cap B^*) \lhd (A^* \cap B^*)$. 同样，$(A^* \cap B) \lhd (A^* \cap B^*)$. 对于子集 $D = (A \cap B^*)(A^* \cap B)$，它是由两个正规子群生成的，所以它是 $A^* \cap B^*$ 的正规子群.

运用注中的对称性，只需证明存在同构

$$\frac{A(A^* \cap B^*)}{A(A^* \cap B)} \to \frac{A^* \cap B^*}{D}.$$

定义 $\varphi: A(A^* \cap B^*) \to (A^* \cap B^*)/D$ 为 $\varphi: ax \mapsto xD$，其中 $a \in A, x \in A^* \cap B^*$. 现在 φ 是合理定义的：如果 $ax = a'x'$，其中 $a' \in A, x' \in A^* \cap B^*$，则 $(a')^{-1}a = x'x^{-1} \in A \cap (A^* \cap B^*) = A \cap B^* \leqslant D$. φ 还是同态：$axa'x' = a''xx'$，其中 $a'' = a(xa'x^{-1}) \in A$（因为 $A \lhd A^*$），从而 $\varphi(axa'x') = \varphi(a''xx') = xx'D = \varphi(ax)\varphi(a'x')$. 容易验证 φ 是满射且 $\ker\varphi = A(A^* \cap B)$. 由第一同构定理即可完成证明. ■

读者可以验证扎森豪斯引理蕴涵第二同构定理：如果 S 和 T 是群 G 的子群满足 $T \lhd G$，则 $TS/T \cong S/(S \cap T)$. 只要令 $A^* = G, A = T, B^* = S$ 和 $B = S \cap T$.

279

定义 **合成列**是指非平凡因子群都是单群的正规列. 合成列的非平凡因子群叫做 G 的**合成因子**.

一个群未必有合成列，例如阿贝尔群$\mathbb{Z}$就没有合成列. 然而，每个有限群都有合成列.

命题 5.50 每个有限群 G 都有合成列.

证明 如果命题不成立，设 G 是最小的出界者；即 G 是没有合成列的阶最小的有限群. 现在 G 不是单群，否则 $G > \{1\}$ 是合成列. 因此 G 有真正规子群 H. 可以假设 H 是一个极大正规子群，从而 G/H 是单群. 而 $|H| < |G|$，所以 H 有合成列，比如 $H = H_0 > H_1 > \cdots > \{1\}$. 但 $G > H_0 > H_1 > \cdots > \{1\}$ 就是 G 的合成列，于是产生矛盾. ■

群 G 是可解的，如果它有正规列且这个正规列的因子群是素数阶循环群. 因素数阶循环群是单

群，所以可解群定义中的正规列是合成列，从而 G 的合成因子是素数阶循环群.

30 阶循环群 $G=\langle a\rangle$ 有两个合成列（注意因为 G 是阿贝尔群，子群的正规性是必然的）. 第一个是

$$G=\langle a\rangle \geqslant \langle a^2\rangle \geqslant \langle a^{10}\rangle \geqslant \{1\};$$

这个合成列的因子群是 $\langle a\rangle/\langle a^2\rangle \cong \mathbb{I}_2, \langle a^2\rangle/\langle a^{10}\rangle \cong \mathbb{I}_5$ 和 $\langle a^{10}\rangle/\{1\} \cong \langle a^{10}\rangle \cong \mathbb{I}_3$. 另一个正规列是

$$G=\langle a\rangle \geqslant \langle a^5\rangle \geqslant \langle a^{15}\rangle \geqslant \{1\};$$

这个正规列的因子群是 $\langle a\rangle/\langle a^5\rangle \cong \mathbb{I}_5, \langle a^5\rangle/\langle a^{15}\rangle \cong \mathbb{I}_3$ 和 $\langle a^{15}\rangle/\{1\} \cong \langle a^{15}\rangle \cong \mathbb{I}_2$. 注意它们生成相同的因子群，虽然生成的次序不同. 我们将看到这个现象是普遍存在的：同一个群的不同合成列有相同的因子群. 这就是若尔当-赫尔德定理，下一定义使得这个定理的陈述更加准确.

定义 群 G 的两个正规列称为**等价**，如果在每个正规列的非平凡因子群的集合之间存在双射使得相应的因子群同构.

若尔当-赫尔德定理说一个群的任两个合成列都是等价的. 证明属于施赖埃尔（Schreier）的更一般的定理比较省事.

280

定义 一个正规列的**加细**是把原始的正规列作为子序列的正规列 $G=N_0, N_1, \cdots, N_k=\{1\}$.

换句话说，一个正规列的加细是在原来的正规列中插进更多的子群形成的一个新的正规列.

注意一个合成列只允许无关紧要的加细，也就是只能插进重复的项（如果 G_i/G_{i+1} 是单群，则它没有真正规子群，因此没有中间子群 L 使得 $G_i>L>G_{i+1}$ 且 $L\lhd G_i$）. 所以任一合成列的加细都等价于原始的合成列.

定理 5.51（施赖埃尔加细定理） 群 G 的任意两个正规列

$$G=G_0 \geqslant G_1 \geqslant \cdots \geqslant G_n=\{1\}$$

和

$$G=N_0 \geqslant N_1 \geqslant \cdots \geqslant N_k=\{1\}$$

有等价的加细.

证明 我们在第一个列的每个相邻对之间插进第二个列的一个复制. 更详细地说，对每个 $i\geqslant 0$，定义

$$G_{ij}=G_{i+1}(G_i \cap N_j)$$

（因为 $G_{i+1}\lhd G_i$，这是一个子群）. 注意，因为 $N_0=G$，所以

$$G_{i0}=G_{i+1}(G_i \cap N_0)=G_{i+1}G_i=G_i,$$

又因为 $N_k=\{1\}$，从而

$$G_{ik}=G_{i+1}(G_i \cap N_k)=G_{i+1},$$

所以，G_{ij} 的列是 G_i 的列的子序列：

$$\cdots \geqslant G_i=G_{i0} \geqslant G_{i1} \geqslant G_{i2} \geqslant \cdots \geqslant G_{ik}=G_{i+1} \geqslant \cdots.$$

同样，子群

$$N_{pq}=N_{p+1}(N_p \cap G_q)$$

形成第二个列的子序列. 两个新的子序列都有 nk 个项. 对每对 i, j 和四个子群 $G_{i+1}\lhd G_i$ 及 $N_{j+1}\lhd N_j$，扎森豪斯引理表明两个子序列都是正规列，因此是加细，且存在同构

$$\frac{G_{i+1}(G_i \cap N_j)}{G_{i+1}(G_i \cap N_{j+1})} \cong \frac{N_{j+1}(N_j \cap G_i)}{N_{j+1}(N_j \cap G_{i+1})};$$

即

$$G_{i,j}/G_{i,j+1} \cong N_{j,i}/N_{j,i+1}.$$

结合 $G_{i,j}/G_{i,j+1} \mapsto N_{j,i}/N_{j,i+1}$ 是双射，它表明两个加细等价. ■ 281

定理 5.52（若尔当-赫尔德[⊖]定理） *一个群 G 的任意两个合成列等价. 特别地，如果合成列存在，则合成列的长度是 G 的不变量.*

证明 我们早先已经注明，合成列的任意加细等价于原始的合成列. 现在由施赖埃尔定理得到任意两个合成列等价. ■

下面是算术基本定理的新证明.

系 5.53 *每个整数 $n \geqslant 2$ 都有素数分解，且素因数由 n 唯一地确定.*

证明 因群 $\mathbb{I}_n$ 是有限群，它有合成列，设 $S_1, \cdots, S_t$ 是因子群. 现在根据命题 2.107，一个阿贝尔群是单群当且仅当它的阶为素数. 因 $n = |\mathbb{I}_n|$ 是因子群的阶之积（见习题 5.36），我们已经证明了 n 是素数的积. 此外，若尔当-赫尔德定理给出因子群的阶（素数）的唯一性. ■

例 5.54 （i）非同构的群可以有相同的合成因子. 例如 $\mathbb{I}_4$ 和 $\mathbf{V}$ 都有因子群为 $\mathbb{I}_2$，$\mathbb{I}_2$ 的合成列.

（ii）设 $G = \mathrm{GL}(2, \mathbb{F}_4)$ 是元素在有四个元素的域 $\mathbb{F}_4$ 中的一切 2×2 非奇异矩阵的一般线性群. 现在，$\det: G \to (\mathbb{F}_4)^{\times}$，其中 $(\mathbb{F}_4)^{\times} \cong \mathbb{I}_3$ 是 $\mathbb{F}_4$ 的非零元素的乘法群. 因 $\ker \det = \mathrm{SL}(2, \mathbb{F}_4)$，就是行列式为 1 的那些矩阵组成的特殊线性群，所以存在正规列

$$G = \mathrm{GL}(2, \mathbb{F}_4) \geqslant \mathrm{SL}(2, \mathbb{F}_4) \geqslant \{1\}.$$

这个正规列的因子群是 $\mathbb{I}_3$ 和 $\mathrm{SL}(2, \mathbb{F}_4)$. $\mathrm{SL}(2, \mathbb{F}_4)$ 是非阿贝尔单群［事实上，系 5.68 说 $\mathrm{SL}(2, \mathbb{F}_4) \cong A_5$］，从而这个正规列是一个合成列. 我们还不能下结论说 G 是不可解的，因为可解性的定义要求有具有素数阶因子群的合成列，但未必是这一个. 然而若尔当-赫尔德定理说如果 G 的一个合成列其因子群都是素数阶的，则其他的每个合成列其因子群也都是素数阶的. 现在可以得出 $\mathrm{GL}(2, \mathbb{F}_4)$ 是不可解群的结论. ■

我们现在讨论若尔当-赫尔德定理在群论中的重要性.

定义 *如果 G 是群且 $K \lhd G$，则 G 称为 K 和 G/K 的扩张.* 282

运用这个术语，习题 2.75 可以表述为一个 p-群和另一个 p-群的扩张也是一个 p-群，命题 4.24 可以表述为一个可解群和另一个可解群的扩张也是一个可解群.

扩张的研究牵涉到反问题：由正规子群 K 和商群 $Q = G/K$ 能够把 G 复原到多大程度？例如，我们知道如果 K 和 Q 是有限的，则 $|G| = |K||Q|$.

例 5.55 （i）直积 $K \times Q$ 是 K 和 Q 的扩张（$K \times Q$ 也是 Q 和 K 的扩张）.

（ii）S_3 和 $\mathbb{I}_6$ 都是 $\mathbb{I}_3$ 和 $\mathbb{I}_2$ 的扩张. 另一方面，$\mathbb{I}_6$ 是 $\mathbb{I}_2$ 和 $\mathbb{I}_3$ 的扩张，而 S_3 不是，因为 S_3 不包含 2 阶正规子群. ■

我们已经看到，对于任意给定的一对群 K 和 Q，K 和 Q 的扩张恒存在（直积），但可能还有不同构于这种扩张的扩张. 因此，如果把 K 和 Q 的扩张看作 K 和 Q 的一个"乘积"，则这个乘积不是单值的. **扩张问题**是对于给定的一对群 K 和 Q 的一切可能的扩张进行分类.

假设群 G 有正规列

$$G = K_0 \geqslant K_1 \geqslant K_2 \geqslant \cdots \geqslant K_{n-1} \geqslant K_n = \{1\},$$

⊖ 1868 年，若尔当证明了合成列的因子群的阶仅依赖于 G 而不依赖于合成列. 1889 年，赫尔德证明如不计同构，则因子群本身不依赖于合成列.

其因子群为 $Q_1,\cdots,Q_n$，其中对一切 $i\geqslant 1$,

$$Q_i = K_{i-1}/K_i.$$

现在 $K_n=\{1\}$，从而 $K_{n-1}=Q_n$，更重要的是：$K_{n-2}/K_{n-1}=Q_{n-1}$，从而 K_{n-2}是 K_{n-1}和 Q_{n-1}的扩张. 如果能够解决扩张问题，则可以从 K_{n-1}和 Q_{n-1}，也就是 Q_n 和 Q_{n-1}取回 K_{n-2}. 下一步考察 $K_{n-3}/K_{n-2}=Q_{n-2}$，从而 K_{n-3}是 K_{n-2}和 Q_{n-2}的扩张. 如果能解决扩张问题，则可以从 K_{n-2}和 Q_{n-2}取回 K_{n-3}，也就是可以从 Q_n，Q_{n-1}和 Q_{n-2}取回 K_{n-3}. 用这种方法沿着合成列向上走，最终 $G=K_0$ 可以从 $Q_n,Q_{n-1},\cdots,Q_1$ 取回. 于是，G 是因子群的“乘积”. 如果正规列是合成列，则若尔当-赫尔德定理说这个乘积的因子（即 G 的合成因子）是被 G 唯一确定的. 所以，如果了解了有限单群且能够解决扩张问题，就能够纵览一切有限群. 在 20 世纪 80 年代对一切有限单群进行了分类，这个定理是数学中最深奥的定理之一，它给出了一切有限单群连同它们的重要性质的一张完整的表. 在某种意义下，扩张问题也已经解决. 在第 10 章中，我们会给出属于施赖埃尔的扩张问题的解，它对于扩张描述了一切可能的乘法表；这个研究导致群的上同调和舒尔-扎森豪斯定理. 另一方面，扩张问题就下面的情况来说还尚未解决：给定 K 和 Q，没有人知道 K 和 Q 的不同构扩张的确切个数的计算方法.

283

我们现在越过一般群（它的合成因子是任意单群）而考察可解群［它的合成因子是素数阶循环群，素数阶循环群总是单群］. 即使可解群是为确定运用根式可解的多项式而产生的，然而有不直接涉及伽罗瓦理论和多项式的关于可解群的纯群论定理. 例如，霍尔（P. Hall）的一个定理推广西罗定理如下：如果 G 是阶为 ab 的可解群，其中 a 和 b 互素，则 G 包含一个 a 阶子群，此外，任意两个这样的子群共轭. 伯恩赛德（W. Burnside）的一个定理说，如果 $|G|=p^mq^n$，其中 p,q 是素数，则 G 是可解群. 值得注意的费特-汤普森（Feit-Thompson）定理说每个奇数阶群必是可解群.

标准群论的构造保持群的可解性. 例如，在命题 4.21 中我们已经看到可解群 G 的每个商群 G/N本身也是可解群，而命题 4.22 表明可解群的每个子群本身也是可解群. 命题 4.24 表明一个可解群和另一个可解群的扩张也是可解群：如果 $H\lhd G$ 且 H 和 G/H 都是可解群，则 G 是可解群. 系 4.25 表明可解群的直积本身是可解群.

命题 5.56 每个有限 p-群是可解群.

证明 如果 G 是阿贝尔群，则 G 是可解群. 否则，如果 G 不是阿贝尔群，根据定理 2.103，它的中心 $Z(G)$ 是非平凡的真正规阿贝尔子群. 现在因为 $Z(G)$ 是阿贝尔群，所以它是可解群，对 $|G|$ 用归纳法可知 $G/Z(G)$ 是可解群，根据命题 4.24，G 是可解群. ■

由此，有限 p-群的直积当然是可解群.

定义 如果 G 是群且 $x,y\in G$，则它们的**换位子** $[x,y]$ 是指元素

$$[x,y]=xyx^{-1}y^{-1}.$$

如果 X 和 Y 是 G 的子群，则$[X,Y]$定义为

$$[X,Y]=\langle [x,y]: x\in X, y\in Y\rangle.$$

特别地，群 G 的**换位子群** G'是指

$$G'=[G,G],$$

即由一切换位子生成的子群[⊖].

⊖ 一切换位子组成的子集未必在乘法下封闭，从而一切换位子的集合可能不是子群. 有两个换位子的积不再是换位子的最小群是 96 阶群. 可参考 297 页上 Carmichael 的习题.

显然群 G 中的两个元素 x 和 y 可交换当且仅当它们的换位子$[x,y]$是 1. 下面的命题推广了这一观察.

284

命题 5.57 设 G 是群.

(i) 换位子群 G' 是 G 的正规子群，且 G/G' 是阿贝尔群.

(ii) 如果 $H \lhd G$ 且 G/H 是阿贝尔群，则 $G' \leqslant H$.

证明 (i) 换位子 $xyx^{-1}y^{-1}$ 的逆本身也是换位子：$[x,y]^{-1} = yxy^{-1}x^{-1} = [y,x]$，所以 G' 的每个元素都是换位子的积. 但任一换位子的共轭也是换位子（因此，换位子的共轭也是换位子的积）：

$$
\begin{aligned}
a[x,y]a^{-1} &= a(xyx^{-1}y^{-1})a^{-1} \\
&= axa^{-1}aya^{-1}ax^{-1}a^{-1}ay^{-1}a^{-1} \\
&= [axa^{-1},aya^{-1}].
\end{aligned}
$$

所以 $G' \lhd G$.（另一种证法：如果 $\varphi: G \to G$ 是同态，则 $\varphi[x,y] = [\varphi(x),\varphi(y)] \in G'$，所以 G' 是 G 的全不变子群.）

如果 $aG',bG' \in G/G'$，则

$$aG'bG'(aG')^{-1}(bG')^{-1} = aba^{-1}b^{-1}G' = [a,b]G' = G',$$

因此 G/G' 是阿贝尔群.

(ii) 假设 $H \lhd G$ 且 G/H 是阿贝尔群. 如果 $a,b \in G$，则 $aHbH=bHaH$，即 $abH=baH$，从而 $b^{-1}a^{-1}ba \in H$. 由于每个换位子都形如 $b^{-1}a^{-1}ba$，所以有 $G' \leqslant H$. ■

例 5.58 (i) 群 G 是阿贝尔群当且仅当 $G' = \{1\}$.

(ii) 如果 G 是单群，因为 G' 是正规子群，所以 $G'=\{1\}$ 或 $G'=G$. 当 G 的阶为素数时，出现第一种情形，否则出现第二种情形. 特别地，对一切 $n \geqslant 5,(A_n)' = A_n$.

(iii) 我们证明对一切 $n \geqslant 5,(S_n)' = A_n$. 因 $S_n/A_n \cong \mathbb{I}_2$ 是阿贝尔群，命题 5.57 表明 $(S_n)' \leqslant A_n$. 关于反包含，注意 $(S_n)' \cap A_n \lhd A_n$，因此 A_n 的单性给出这个交是平凡的或者是 A_n. 显然，$(S_n)' \cap A_n \neq \{(1)\}$，所以 $A_n \leqslant (S_n)'$. ■

我们迭代换位子群.

定义 G 的导出列是指

$$G = G^{(0)} \geqslant G^{(1)} \geqslant G^{(2)} \geqslant \cdots \geqslant G^{(i)} \geqslant G^{(i+1)} \geqslant \cdots,$$

其中 $G^{(0)} = G, G^{(1)} = G'$，更一般地，对一切 $i \geqslant 0, G^{(i+1)} = (G^{(i)})' = [G^{(i)},G^{(i)}]$.

285

对 $i \geqslant 0$ 用归纳法容易证明 $G^{(i)}$ 是全不变子群，由此蕴涵 $G^{(i)} \lhd G$，从而 $G^{(i+1)} \lhd G^{(i)}$，所以导出列是正规列. 导出列可以用来给出可解性的一个刻画：G 是**可解**的当且仅当导出列达到$\{1\}$.

命题 5.59 (i) 有限群 G 是可解群当且仅当它有正规列，且其因子群为阿贝尔群.

(ii) 有限群 G 是可解群当且仅当存在某个 n 使得

$$G^{(n)} = \{1\}.$$

证明 (i) 如果 G 是可解群，则 G 有一个正规列，它的一切因子群 G_i/G_{i+1} 都是素数阶循环群，因此是阿贝尔群.

反之，如果 G 有因子群都是阿贝尔群的正规列，则任一加细的因子群也是阿贝尔群. 特别地，因 G 是有限群，存在 G 的合成列，这个合成列的因子群是阿贝尔单群，因此，它们是素数阶循环群，从而 G 是可解的.

(ii) 假定 G 是可解群，于是存在正规列

$$G \geqslant G_1 \geqslant G_2 \geqslant \cdots \geqslant G_n = \{1\},$$

它的因子群 G_i/G_{i+1} 是阿贝尔群. 对 $i \geqslant 0$ 用归纳法证明 $G^{(i)} \leqslant G_i$. 因 $G^{(0)}=G=G_0$，基础步显然成立. 关于归纳步，因 G_i/G_{i+1} 是阿贝尔群，命题 5.57 给出 $(G_i)' \leqslant G_{i+1}$. 另一方面，归纳假设给出 $G^{(i)} \leqslant G_i$，它蕴涵

$$G^{(i+1)} = (G^{(i)})' \leqslant (G_i)' \leqslant G_{i+1}.$$

特别地，$G^{(n)} \leqslant G_n = \{1\}$，这正是我们想要证明的.

反之，如果 $G^{(n)}=\{1\}$，则导出列是正规列（一个正规列必终止于 $\{1\}$）且具有阿贝尔因子群，因此（i）给出 G 可解. ■

例如，易知 $G=S_4$ 的导出列是

$$S_4 > A_4 > \mathbf{V} > \{(1)\}.$$

我们早先的可解性的定义只适用于有限群，而命题中的刻画对一切群（可以是无限群）都有意义. 今天大多数作者把一个群的导出列经有限步后达到 $\{1\}$ 作为可解群的定义. 根据这个新定义，每个阿贝尔群都是可解群，而在原来的定义下，阿贝尔群是可解的当且仅当它们是有限的. 习题 5.38 中，要求读者用命题 5.59 的准则证明可解群的子群、商群和扩张也是可解的（在新的、推广的意义下）.

[286] 用正规列还定义了其他重要群类，其中最重要的一个是由幂零群组成的.

定义 *群 G 的***降中心列***是指*

$$G = \gamma_1(G) \geqslant \gamma_2(G) \geqslant \cdots,$$

*其中 $\gamma_{i+1}(G) = [\gamma_i(G), G]$. 群 G 称为***幂零群***，如果降中心列达到 $\{1\}$，即对某个 n 有 $\gamma_n(G) = \{1\}$.*

注意 $\gamma_2(G) = G'$，但随后导出列和降中心列可能不同，例如 $\gamma_3(G) = [G', G] \geqslant G^{(2)}$，且严格的不等性是可能的.

有限幂零群可以用命题 5.39 来刻画：这种群是它们的西罗子群的直积，从而可以把有限幂零群看作广义 p-群. $\mathrm{UT}(n, \mathbb{F}_q)$、$\mathrm{UT}(n, \mathbb{Z})$（$\mathbb{Z}$ 上的幺三角矩阵群）、有限群 G 的费拉蒂尼（Frattini）子群 $\Phi(G)$（在习题 5.46 中定义）以及从一个群的正规列产生的某种自同构群都是幂零群的例子. 我们可以对无限幂零群证明结果，也可以对有限幂零群证明结果，如习题 5.47 中的那些结论：有限幂零群 G 的每个子群和每个商群也是幂零群；如果 $G/Z(G)$ 是幂零群，则 G 也是幂零群；每个正规子群 H 非平凡地与 $Z(G)$ 相交.

习题

5.33 设 p 是素数且 G 是 p^3 阶非阿贝尔群. 证明 $Z(G) = G'$.

提示：先证明两个子群的阶都是 p.

5.34 证明：如果 H 是群 G 的子群且 $G' \leqslant H$，则 $H \lhd G$.

提示：用对应定理.

5.35 （i）对 $n = 2,3,4$，证明 $(S_n)' = A_n$ [对 $n \geqslant 5$，见例5.58(iii)].

（ii）证明 $(\mathrm{GL}(n,k))' \leqslant \mathrm{SL}(n,k)$.（反包含也成立. 对 $n=2$ 的情形，见习题 5.56.）

5.36 如果 G 是有限群且

$$G = G_0 \geqslant G_1 \geqslant \cdots \geqslant G_n = \{1\}$$

是正规列，证明 G 的阶是因子群的阶之积：

$$|G|=\prod_{i=0}^{n-1}|G_i/G_{i+1}|.$$

5.37 证明任意两个同阶有限可解群有相同的合成因子.

5.38 设 G 是任意群，可以是无限群.

(i) 证明：如果 $H\leqslant G$，则对一切 i，$H^{(i)}\leqslant G^{(i)}$. 运用命题 5.59 可知可解群的每个子群也是可解群.

(ii) 证明：如果 $f: G\to K$ 是满同态，则对一切 i，

$$f(G^{(i)})=K^{(i)}.$$

运用命题 5.59 可知可解群的每个商群也是可解群.

287

(iii) 对每个群 G，用双重归纳法证明

$$G^{(m+n)}=(G^{(m)})^{(n)}.$$

(iv) 用命题 5.59 证明：如果 $H\lhd G$ 且 H 和 G/H 都是可解群，则 G 是可解群.

5.39 设 p 和 q 是素数.

(i) 证明每个 pq 阶群都是可解群.

提示：如果 $p=q$，则 G 是阿贝尔群. 如果 $p<q$，则 pq 的因数 r 满足 $r\equiv 1 \bmod q$ 必等于 1.

(ii) 证明每个 p^2q 阶群 G 是可解群.

提示：如果 G 不是单群，用命题 4.24. 如果 $p>q$，则 $r\equiv 1 \bmod p$ 迫使 $r=1$. 如果 $p<q$，则 $r=p^2$ 且 G 中存在多于 p^2q 个元素.

5.40 证明费特-汤普森定理"每个奇数阶有限群都是可解群"等价于"每个非阿贝尔有限群的阶为偶数".

提示：对于充分性，选取"最小的出界者"：阶为最小奇数的非可解群 G. 由假设，G 不是单群，从而它有非平凡的真正规子群.

5.41 (i) 证明无限循环群$\mathbb{Z}$没有合成列.

(ii) 证明阿贝尔群 G 有合成列当且仅当 G 是有限群.

5.42 证明：如果 G 是有限群且 $H\lhd G$，则存在 G 的这样的合成列，其中有一项是 H.

提示：用施赖埃尔定理.

5.43 (i) 证明：如果 S 和 T 是群 G 的可解子群，且 $S\lhd G$，则 ST 也是 G 的可解子群.

提示：子群 ST 是 $S\times T$ 的同态象.

(ii) 如果 G 是有限群，定义 $\mathcal{S}(G)$ 为由 G 的一切正规可解子群生成的 G 的子群. 证明 $\mathcal{S}(G)$ 是 G 的唯一的极大正规可解子群且 $G/\mathcal{S}(G)$ 没有非平凡的正规可解子群.

5.44 (i) 证明二面体群 D_{2n} 是可解群.

(ii) 求 D_{2n} 的一个合成列.

5.45 (Rosset) 设 G 是群，它包含元素 x, y 使得 x，y 和 xy 的阶两两互素，证明 G 不是可解群.

5.46 (i) 如果 G 是有限群，定义它的**弗拉蒂尼子群**为 G 的一切极大子群的交，记为 $\Phi(G)$. 证明 $\Phi(G)$ 是一个特征子群，因此它是 G 的正规子群.

(ii) 证明：如果 p 是素数且 G 是有限阿贝尔 p-群，则 $\Phi(G)=pG$. **伯恩赛德** (Burnside) **基定理**说，如果 G 是任意（不必是阿贝尔群）有限 p-群，则 $G/\Phi(G)$ 是$\mathbb{F}_p$ 上的向量空间，它的维数是 G 的生成元的最少个数.（见罗特曼所著的《An Introduction to the Theory of Groups》124 页）.

5.47 (i) 如果 G 是幂零群，证明它的中心 $Z(G)\neq\{1\}$.

(ii) 如果 G 是群且 $G/Z(G)$ 是幂零群，证明 G 是幂零群.

(iii) 如果 G 是幂零群，证明 G 的每个子群和商群也都是幂零群.

288

(iv) 设 G 是群且 $H\lhd G$. 举出一个例子使得 H 和 G/H 都是幂零群而 G 不是幂零群.

(v) 如果 G 是有限 p-群且 $H\lhd G$，证明 $H\cap Z(G)\neq\{1\}$.（将这个结果推广到有限幂零群也成立.）

5.48 用 $\mathfrak{A}$ 表示一切阿贝尔群的类，用 $\mathfrak{N}$ 表示一切幂零群的类，用 $\mathfrak{S}$ 表示一切可解群的类.

(i) 证明 $\mathfrak{A}\subseteq\mathfrak{N}\subseteq\mathfrak{S}$.

(ii) 证明 (i) 中的每个包含关系都是严格的，即存在不是阿贝尔群的幂零群，并且存在不是幂零群的可解群.

5.49 如果 G 是群且 $g,x\in G$，记 $g^x=xgx^{-1}$.

(i) 证明对一切 $x,y,z\in G,[x,yz]=[x,y][x,z]^y$ 和 $[xy,z]=[y,z]^x[x,z]$.

(ii)（雅可比 (Jacobi) 恒等式）设 $x,y,z\in G$ 是群 G 的元素，定义

$$[x,y,z]=[x,[y,z]].$$

证明

$$[x,y^{-1},z]^y[y,z^{-1},x]^z[z,x^{-1},y]^x=1.$$

5.50 如果 H,K,L 是群 G 的子群，定义

$$[H,K,L]=\langle\{[h,k,\ell]:h\in H,k\in K,\ell\in L\}\rangle.$$

(i) 证明：如果 $[H,K,L]=\{1\}=[K,L,H]$，则 $[L,H,K]=\{1\}$.

(ii)（三子群引理）如果 $N\triangleleft G$ 且 $[H,K,L][K,L,H]\leqslant N$，证明

$$[L,H,K]\leqslant N.$$

(iii) 证明：如果 G 是群且 $G=G'$，则 $G/Z(G)$ 无中心.

提示： 如果 $\pi:G\to G/Z(G)$ 是自然映射，定义 $\zeta^2(G)=\pi^{-1}(Z(G/Z(G)))$. 用三子群引理以及 $L=\zeta^2(G)$ 和 $H=K=G$.

(iv) 证明对一切 i，j 有 $[\gamma_i(G),\gamma_j(G)]\leqslant\gamma_{i+j}(G)$.

5.4 射影幺模群

若尔当-赫尔德定理把一个单群族和每个有限群联系起来，它可以把许多关于有限群的问题简化为有限单群的问题. 这一经验事实说明了解单群是十分有用的. 至今我们知道的单群只有素数阶循环群和对 $n\geqslant5$ 的交错群 A_n，我们现在要证明某种矩阵的有限群是单群，一开始先考虑某些矩阵，它们在 2×2 线性群中扮演的角色如同交错群中 3-轮换扮演的角色. [289]

定义 域 k 上的一个平延[⊖]是指形如

$$B_{12}(r)=\begin{bmatrix}1&r\\0&1\end{bmatrix}\quad 或\quad B_{21}(r)=\begin{bmatrix}1&0\\r&1\end{bmatrix}$$

的矩阵，其中 $r\in k$ 且 $r\neq0$.

设 A 是 2×2 矩阵. 易知 $B_{12}(r)A$ 是把 A 的 Row(1) 换成 Row(1) + r Row(2) 得到的矩阵，$B_{21}(r)A$ 是把 A 的 Row(2) 换成 Row(2) + r Row(1) 得到的矩阵.

引理 5.60 设 k 是域且 $A\in\mathrm{GL}(2,k)$，则

$$A=UD,$$

其中 U 是平延的积，$D=\mathrm{diag}\{1,d\}=\begin{bmatrix}1&0\\0&d\end{bmatrix}$，其中 $d=\det(A)$.

⊖ 多数群论学家定义 2×2 平延是相似于 $B_{12}(r)$ 或 $B_{21}(r)$ 的矩阵［即 $B_{12}(r)$ 或 $B_{21}(r)$ 在 GL(2,k) 中的共轭］. Transvection（平延）这个字是 transporting（传送）的同义词，它在这个上下文中的用法可能属于阿廷 (E. Artin)，他在他的书《Geometric Algebra》中给出下面的定义："如果 V 是 n 维向量空间，称一个元素 $\tau\in\mathrm{GL}(V)$ 为一个平延，如果它保持某个超平面 H 的每个向量不变，而任一向量 $x\in V$ 都被 H 的某个向量移动，即 $\tau(x)-x\in H$." 在我们的情形中，$B_{12}(r)$ 固定 "x-轴"，$B_{21}(r)$ 固定 "y-轴."

证明 设

$$A=\begin{bmatrix}p & q\\ r & s\end{bmatrix}.$$

可以假设 $r\neq 0$，否则 $p\neq 0$（因为 A 是非奇异的），把 Row(2) 换成 Row(2)＋Row(1) 就把 p 放到了 21 位置．接下来，把 Row(1) 换成 Row(1)$+r^{-1}(1-p)$Row(2)，从而 1 在左上角．现在继续乘以平延：

$$\begin{bmatrix}1 & x\\ r & s\end{bmatrix}\to\begin{bmatrix}1 & x\\ 0 & y\end{bmatrix}\to\begin{bmatrix}1 & 0\\ 0 & d\end{bmatrix}.$$

于是 $WA=D$，其中 W 是平延的积且 $D=\operatorname{diag}\{1,d\}$．因平延的行列式为 1，所以 $\det(W)=1$，从而

$$\det(A)=\det(D)=d.$$

因平延的逆也是平延，所以有 $A=W^{-1}D$，它就是我们要找的因子分解． ■

回忆 $SL(2,k)$ 是 $GL(2,k)$ 的子群，它由一切行列式为 1 的矩阵组成[⊖]．如果 k 是有限域，则 $k\cong\mathbb{F}_q$，其中 $q=p^n$ 且 p 是素数，可以记 $GL(2,\mathbb{F}_q)$ 为 $GL(2,q)$，同样，可以记 $SL(2,\mathbb{F}_q)$ 为 $SL(2,q)$． [290]

命题 5.61 （ⅰ）如果 k 是域，则 $SL(2,k)$ 由平延生成．

（ⅱ）如果 k 是域，则 $GL(2,k)/SL(2,k)\cong k^{\times}$，其中 $k^{\times}$ 是 k 的非零元素的乘法群．

（ⅲ）如果 $k=\mathbb{F}_q$，则

$$|SL(2,\mathbb{F}_q)|=(q+1)q(q-1).$$

证明 （ⅰ）如果 $A\in SL(2,k)$，则引理 5.60 给出因子分解 $A=UD$，其中 U 是平延的积，$D=\operatorname{diag}\{1,d\}$，其中 $d=\det(A)$．因 $A\in SL(2,k)$，因此有 $\det(A)=1$，所以 $A=U$．

（ⅱ）如果 $a\in k^{\times}$，则矩阵 $\operatorname{diag}\{1,a\}$ 的行列式为 a，因此是非奇异的，从而映射 $\det: GL(2,k)\to k^{\times}$ 是满射．$SL(2,k)$ 的定义表明它是 det 的核，因此由第一同构定理可得结果．

（ⅲ）如果 H 是有限群 G 的正规子群，则拉格朗日定理给出 $|H|=|G|/|G/H|$．特别地，

$$|SL(2,\mathbb{F}_q)|=|GL(2,\mathbb{F}_q)|/|\mathbb{F}_q^{\times}|.$$

而由定理 5.46，$|GL(2,\mathbb{F}_q)|=(q^2-1)(q^2-q)$，又 $|\mathbb{F}_q^{\times}|=q-1$，因此，$|SL(2,\mathbb{F}_q)|=(q+1)q(q-1)$． ■

我们现在计算这些矩阵群的中心．如果 V 是 k 上的二维向量空间，则在命题 3.108 中已经证明了 $GL(2,k)\cong GL(V)$，它是 V 上一切非奇异线性变换组成的群．此外，命题3.109(ⅰ)把中心和标量变换等同起来．

命题 5.62 $SL(2.k)$ 的中心由一切满足 $a^2=1$ 的标量矩阵 $\begin{bmatrix}a & 0\\ 0 & a\end{bmatrix}$ 组成，记为 $SZ(2,k)$．

注 这里我们看到 $SZ=SL\cap Z(GL)$，但在一般情形下，命题"如果 $H\leqslant G$，则 $Z(H)=H\cap Z(G)$"不成立（确实，即使 H 是正规子群，这个等式也可能不成立）．我们恒有 $H\cap Z(G)\leqslant Z(H)$，但包含可以是严格的．例如，如果 $G=S_3$ 和 $H=A_3\cong\mathbb{I}_3$，则 $Z(A_3)=A_3$ 而 $A_3\cap Z(S_3)=\{1\}$．

证明 这里用线性变换比用矩阵更方便．假定 $T\in SL(2,k)$ 不是标量变换，于是存在非零向量 $v\in V$ 使得 Tv 不是 v 的标量倍，由此 v,Tv 线性无关，因 $\dim(V)=2$，所以 v,Tv 是 V 的一组基．定义 $S: V\to V$ 为 $S(v)=v$ 和 $S(Tv)=v+Tv$．注意 S 关于基 v,Tv 有矩阵 $B_{12}(1)$，从而 $\det(S)=1$．

⊖ GL 是 general linear（一般线性）的缩写，SL 是 special linear（特殊线性）的缩写．

现在因为 $TS(v)=Tv$ 而 $ST(v)=v+Tv$，所以 T 和 S 不交换．由此中心必由标量变换组成．用矩阵的话说，中心由标量矩阵 $A=\mathrm{diag}\{a,a\}$ 组成，其中 $a^2=\det(A)=1$. ■

291

定义 射影幺模群[1]是指商群

$$\mathrm{PSL}(2,k)=\mathrm{SL}(2,k)/\mathrm{SZ}(2,k).$$

注意，如果 $c^2=1$，其中 c 在一个域 k 中，则 $c=\pm 1$. 如果 $k=\mathbf{F}_q$，其中 q 是 2 的幂，则 $\mathbf{F}_q$ 有特征 2，从而 $c^2=1$ 蕴涵 $c=1$. 所以在这种情形下，$\mathrm{SZ}(2,\mathbf{F}_q)=\{I\}$，从而 $\mathrm{PSL}(2,\mathbf{F}_{2^n})=\mathrm{SL}(2,\mathbf{F}_{2^n})$.

命题 5.63

$$|\mathrm{PSL}(2,\mathbf{F}_q)|=\begin{cases}\frac{1}{2}(q+1)q(q-1) & \text{如果 } q=p^n \text{ 且 } p \text{ 是奇素数；}\\ (q+1)q(q-1) & \text{如果 } q=2^n.\end{cases}$$

证明 命题5.61(ⅲ)给出 $|\mathrm{PSL}(2,\mathbf{F}_q)|=(q+1)q(q-1)/|\mathrm{SZ}(2,\mathbf{F}_q)|$，命题 5.62 给出

$$|\mathrm{SZ}(2,\mathbf{F}_q)|=|\{a\in\mathbf{F}_q : a^2=1\}|.$$

现在根据定理 3.30，$\mathbf{F}_q^\times$ 是 $q-1$ 阶循环群．如果 q 是奇数，则 $q-1$ 是偶数，循环群 $\mathbf{F}_q^\times$ 有唯一的 2 阶子群；如果 q 是 2 的幂，则我们注意到刚才在这个命题陈述之前，有 $\mathrm{SZ}(2,\mathbf{F}_q)=\{I\}$．所以，如果 q 是奇素数的幂，则 $|\mathrm{SZ}(2,q)|=2$，如果 q 是 2 的幂，则 $|\mathrm{SZ}(2,q)|=1$. ■

现在要证明对一切素数幂 $q\geqslant 4$，群 $\mathrm{PSL}(2,\mathbf{F}_q)$ 都是单群．如同我们早先说的，平延扮演了 3-轮换的角色（见习题 2.91）．

引理 5.64 如果 H 是 $\mathrm{SL}(2,\mathbf{F}_q)$ 的正规子群，且包含一个平延 $B_{12}(r)$ 或 $B_{21}(r)$，则 $H=\mathrm{SL}(2,\mathbf{F}_q)$．

证明 首先注意到，如果

$$U=\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix},$$

则 $\det(U)=1$，从而 $U\in\mathrm{SL}(2,\mathbf{F}_q)$．因 H 是正规子群，$UB_{12}(r)U^{-1}$ 也在 H 中．而 $UB_{12}(r)U^{-1}=B_{21}(-r)$，因此 H 包含形如 $B_{12}(r)$ 的平延当且仅当它包含形如 $B_{21}(-r)$ 的平延．因 SL 是由平延生成的，所以只需证明每个平延 $B_{12}(r)$ 都在 H 中．

因 H 是正规子群，所以 $B_{12}(r)$ 的如下共轭在 H 中：

$$\begin{bmatrix}\alpha & \beta\\ 0 & \alpha^{-1}\end{bmatrix}\begin{bmatrix}1 & r\\ 0 & 1\end{bmatrix}\begin{bmatrix}\alpha^{-1} & -\beta\\ 0 & \alpha\end{bmatrix}=\begin{bmatrix}1 & r\alpha^2\\ 0 & 1\end{bmatrix}=B_{12}(r\alpha^2).$$

定义

292

$$G=\{0\}\cup\{u\in\mathbf{F}_q : B_{12}(u)\in H\}.$$

刚才已经证明对一切 $\alpha\in\mathbf{F}_q$，$r\alpha^2\in G$. 容易验证 G 是加法群 $\mathbf{F}_q$ 的子群，因此它包含形如 $u=r(\alpha^2-\beta^2)$ 的一切元素，其中 $\alpha,\beta\in\mathbf{F}_q$．我们断言 $G=\mathbf{F}_q$，从而完成证明．

如果 q 是奇数，则每个 $w\in\mathbf{F}_q$ 都是一个平方差：

$$w=\left[\frac{1}{2}(w+1)\right]^2-\left[\frac{1}{2}(w-1)\right]^2.$$

因此，如果 $u\in\mathbf{F}_q$，则存在 $\alpha,\beta\in\mathbf{F}_q$ 使得 $r^{-1}u=\alpha^2-\beta^2$，从而 $u=r(\alpha^2-\beta^2)\in G$，所以 $G=\mathbf{F}_q$. 如果 $q=2^m$，则函数 $u\mapsto u^2$ 是单射 $\mathbf{F}_q\to\mathbf{F}_q$（因为如果 $u^2=v^2$，则 $0=u^2-v^2=(u-v)^2$，从而

[1] 行列式为 1 的矩阵称为幺模矩阵．加上形容词射影是因为这个群由射影平面的自同构组成．

$u=v$). 根据习题 1.58（从一个有限集到它自身的单射必是双射），这个函数是满射，因此每个元素 u 都有一个平方根在$\mathbb{F}_q$ 中，特别是存在 $\alpha\in\mathbb{F}_q$ 使得 $r^{-1}u=\alpha^2$，从而 $u=r\alpha^2\in G$. ■

在给出主要结果之前，我们还需要一个短的技术性引理.

引理 5.65 设 H 是 $\mathrm{SL}(2,\mathbb{F}_q)$ 的正规子群. 如果 $A\in H$ 相似于

$$R=\begin{bmatrix}\alpha & \beta\\ \gamma & \delta\end{bmatrix},$$

其中 $R\in\mathrm{GL}(2,\mathbb{F}_q)$，则存在 $u\in\mathbb{F}_q$ 使得 H 包含

$$\begin{bmatrix}\alpha & u^{-1}\beta\\ u\gamma & \delta\end{bmatrix}.$$

证明 由假设，存在矩阵 $P\in\mathrm{GL}(2,\mathbb{F}_q)$ 使得 $R=PAP^{-1}$. 根据引理 5.60，存在矩阵 $U\in\mathrm{SL}$ 和对角矩阵 $D=\mathrm{diag}\{1,u\}$ 使得 $P^{-1}=UD$. 所以，$A=UDRD^{-1}U^{-1}$. 因 $H\lhd\mathrm{SL}$，我们有 $DRD^{-1}=U^{-1}AU\in H$. 但

$$DRD^{-1}=\begin{bmatrix}1 & 0\\ 0 & u\end{bmatrix}\begin{bmatrix}\alpha & \beta\\ \gamma & \delta\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & u^{-1}\end{bmatrix}=\begin{bmatrix}\alpha & u^{-1}\beta\\ u\gamma & \delta\end{bmatrix}.$$ ■

若尔当在 1870 年对 q 是素数的情形证明了下一定理. 1893 年科尔（F. Cole）发现了一个 504 阶单群之后，穆尔认识到科尔群与 $\mathrm{PSL}(2,\mathbb{F}_8)$ 相同，然后他对一切素数幂 $q\geqslant 4$ 证明了 $\mathrm{PSL}(2,\mathbb{F}_q)$ 的单性. 对一切 $m\geqslant 3$，可以定义 $\mathrm{PSL}(m,\mathbb{F}_q)$ 为 $\mathrm{SL}(m,\mathbb{F}_q)/\mathrm{SZ}(m,\mathbb{F}_q)$，若尔当证明了对一切 $m\geqslant 3$ 和一切素数 p, $\mathrm{PSL}(m,\mathbb{F}_p)$ 是单群. 1897 年，迪克森（L. E. Dickson）证明了对一切素数幂 q, $\mathrm{PSL}(m,\mathbb{F}_q)$ 是单群.

我们要用到系 3.101：域 k 上的两个 $n\times n$ 矩阵 A 和 B 相似（即存在非奇异矩阵 P 使得 $B=PAP^{-1}$）当且仅当它们是同一线性变换 $\varphi: k^n\to k^n$ 在 k^n 的两个基下的矩阵. 当然域 k 上的两个非奇异 $n\times n$ 矩阵 A 和 B 相似当且仅当它们是群 $\mathrm{GL}(n,k)$中的共轭元素.

293

定理 5.66（若尔当-穆尔） 对一切素数幂 $q\geqslant 4$，群 $\mathrm{PSL}(2,\mathbb{F}_q)$ 都是单群.

注 由命题 5.63，$|\mathrm{PSL}(2,\mathbb{F}_2)|=6$ 和 $|\mathrm{PSL}(2,\mathbb{F}_3)|=12$，所以这两个群没有一个是单群.

对每个无限域 k, $\mathrm{PSL}(2,k)$ 是单群.

证明 只需证明 $\mathrm{SL}(2,\mathbb{F}_q)$ 的一个包含不在中心 $\mathrm{SZ}(2,\mathbb{F}_q)$ 中的矩阵的正规子群 H 必是整个 $\mathrm{SL}(2,\mathbb{F}_q)$.

先假设 H 包含矩阵

$$A=\begin{bmatrix}\alpha & 0\\ \beta & \alpha^{-1}\end{bmatrix},$$

其中 $\alpha\neq\pm1$；即 $\alpha^2\neq 1$. 如果 $B=B_{21}(1)$，则 H 包含换位子 $BAB^{-1}A^{-1}=B_{21}(1-\alpha^{-2})$，因为 $1-\alpha^{-2}\neq 0$，所以它是平延，从而根据引理 5.64，$H=\mathrm{SL}(2,\mathbb{F}_q)$.

为完成证明，只需证明 H 包含一个第一行是 $[\alpha\ 0]$ 的矩阵，其中 $\alpha\neq\pm1$. 由假设，存在某个非标量矩阵 $M\in H$. 令 $\varphi: k^2\to k^2$ 是由 $\varphi(v)=Mv$ 给出的线性变换，其中 v 是一个 2×1 列向量. 如果对一切 v, $\varphi(v)=c_v v$，其中 $c_v\in k$，则在 k^2 的任意一个基下，矩阵 $[\varphi]$ 都是对角矩阵. 在这种情形下，M 相似于对角矩阵 $D=\mathrm{diag}\{\alpha,\beta\}$，引理 5.65 说 $D\in H$. 因 $M\notin\mathrm{SZ}(2,\mathbb{F}_q)$，必有 $\alpha\neq\beta$. 但 $\alpha\beta=\det(M)=1$，从而 $\alpha\neq\pm1$. 所以 D 是 H 中的一个我们想要的那种形式的矩阵.

剩下的情形是存在向量 v 使得 $\varphi(v)$ 不是 v 的标量倍，在例3.96(ii)中我们看到 M 相似于形如

$$\begin{bmatrix} 0 & -1 \\ 1 & b \end{bmatrix}$$

的矩阵（所以有这种形式是因为它的行列式为 1）. 现在引理 5.65 说存在某个 $u \in k$ 使得

$$D = \begin{bmatrix} 0 & -u^{-1} \\ u & b \end{bmatrix} \in H.$$

如果 $T = \mathrm{diag}\{\alpha, \alpha^{-1}\}$（其中 α 将在稍后取定），则换位子

$$V = (TDT^{-1})D^{-1} = \begin{bmatrix} \alpha^2 & 0 \\ ub(\alpha^{-2} - 1) & \alpha^{-2} \end{bmatrix} \in H.$$

如果 $\alpha^2 \neq \pm 1$；即如果存在某个 $\alpha \in k$ 使得 $\alpha^4 \neq 1$，证明已经完成. 如果 $q > 5$，则因为多项式 $x^4 - 1$ 在一个域中最多有四个根，所以这样的元素 α 是存在的. 如果 $q = 4$，则每个 $\alpha \in \mathrm{F}_4$ 都是方程 $x^4 - x$ 的根，从而 $\alpha \neq 1$ 蕴涵 $\alpha^4 \neq 1$.

294

只剩下 $q = 5$ 的情形. D 中的元素 b 出现在换位子 V 的左下角 $v = ub(\alpha^{-2} - 1)$ 之中. 分 $b \neq 0$ 和 $b = 0$ 两种情形. 在第一种情形中，选取 $\alpha = 2$，从而 $\alpha^{-2} = 4 = \alpha^2$ 且 $v = (4-1)ub = 3ub \neq 0$. 现在 H 包含 $V^2 = B_{21}(-2v)$，因为 $-2v = -6ub = 4ub \neq 0$，所以 V^2 是平延. 最后，如果 $b = 0$，则 D 形如

$$D = \begin{bmatrix} 0 & -u^{-1} \\ u & 0 \end{bmatrix}.$$

对 $y \in \mathrm{F}_5$ 用 $B_{12}(y)$ 作 D 的共轭，得矩阵 $B_{12}(y)DB_{12}(-y) \in H$，它的第一行是

$$[uy \quad uy^2 - u^{-1}].$$

如果选取 $y = 2u^{-1}$，则第一行为 $[2\ 0]$，证明完成. ■

下面是这些单群中起先几个的阶：

$$|\mathrm{PSL}(2, \mathrm{F}_4)| = 60;$$
$$|\mathrm{PSL}(2, \mathrm{F}_5)| = 60;$$
$$|\mathrm{PSL}(2, \mathrm{F}_7)| = 168;$$
$$|\mathrm{PSL}(2, \mathrm{F}_8)| = 504;$$
$$|\mathrm{PSL}(2, \mathrm{F}_9)| = 360;$$
$$|\mathrm{PSL}(2, \mathrm{F}_{11})| = 660.$$

可以证明没有阶在 60 和 168 之间的非阿贝尔单群. 其实，这些就是所有阶小于 1 000 的非阿贝尔单群.

表中的有些阶（即 60 和 360）和交错群的阶一样. 存在阶相同而不同构的单群，例如 A_8 和 $\mathrm{PSL}(3, \mathrm{F}_4)$ 就是阶为 $\frac{1}{2}8! = 20\,160$ 的不同构的单群. 下一结果证明任意两个 60 阶单群同构［习题 5.53 证明 $\mathrm{PSL}(2, \mathrm{F}_9) \cong A_6$］.

命题 5.67 *如果 G 是 60 阶单群，则 $G \cong A_5$.*

证明 只要证明 G 有指数为 5 的子群，因为由定理 2.88，在 H 的陪集上的表示给出同态 $\varphi: G \to S_5$ 使得 $\ker\varphi \leqslant H$. 因 G 是单群，真正规子群 $\ker\varphi$ 等于 $\{1\}$，从而 G 同构于 S_5 的 60 阶子群. 根据习题2.94(ii)，S_5 的 60 阶子群只有 A_5，所以 $G \cong A_5$.

假设 P 和 Q 是 G 的西罗 2-子群满足 $P \cap Q \neq \{1\}$；选取 $x \in P \cap Q$ 且 $x \neq 1$. 现在 P 的阶为 4，因此是阿贝尔群，由拉格朗日定理，$4 \mid |C_G(x)|$. 事实上，因 P 和 Q 两个都是阿贝尔群，子集

$P \cup Q$ 包含在 $C_G(x)$ 中，从而 $|C_G(x)| \geqslant |P \cup Q| > 4$. 所以 $|C_G(x)|$ 是 4 的真倍数，它也是 60 的因数：或者 $|C_G(x)| = 12$，或者 $|C_G(x)| = 20$，或者 $|C_G(x)| = 60$. 第二种情形不可能发生，否则 $C_G(x)$ 的指数为 3，G 在它的陪集上的表示证明 G 同构于 S_3 的子群．第三种情形也不可能发生，否则 $x \in Z(G) = \{1\}$. 因此 $C_G(x)$ 是 G 的指数为 5 的子群，且在这种情形下，我们的证明已经完成．现在可以假定 G 的每一对西罗 2-子群交于 $\{1\}$. [295]

G 的一个西罗 2-子群 P 有 $r = [G: N_G(P)]$ 个共轭，其中 $r = 3,5$ 或 15. 现在 $r \neq 3$（G 没有指数为 3 的子群）．我们用计算元素个数的方法证明 $r=15$ 是不可能的．每个西罗 2-子群包含三个非幺元元素．因任两个西罗 2-子群的交是平凡子群（有如我们在上面看到的），它们的并包含 $15 \times 3 = 45$ 个非幺元元素．现在 G 的一个西罗 5-子群必有 6 个共轭（它们的个数 r_5 是 60 的因数且满足 $r_5 \equiv 1 \bmod 5$）．而西罗 5-子群是 5 阶循环群，所以它们任一对的交为 $\{1\}$，从而它们的并包含 $6 \times 4 = 24$ 个非幺元元素．我们算出的数目已经超过了 G 元素的个数，所以这种情形不可能发生． ■

系 5.68 $\mathrm{PSL}(2,\mathbb{F}_4) \cong A_5 \cong \mathrm{PSL}(2,\mathbb{F}_5)$.

证明 三个群都是单群且阶都是 60. ■

还有其他单矩阵群的无限族（除了素数阶循环群、交错群和射影幺模群之外），以及 26 个零星单群属于非无限的族，最大的一个是阶近似于 8.08×10^{53} 的"怪物"．对感兴趣的读者我们推荐 E. Artin, R. Carter 和 J. Dieudonné 的书．事实上，20 世纪 80 年代给出了一切有限单群的分类，对于这个分类的一个极好的记述可以在 Conway 等所著的《ATLAS of Finite Groups》中找到．

习题

5.51 给出 $\mathrm{GL}(2,\mathbb{F}_5)$ 的合成列，并列出它的因子群．

5.52 （i）证明 $\mathrm{PSL}(2,\mathbb{F}_2) \cong S_3$.

（ii）证明 $\mathrm{PSL}(2,\mathbb{F}_3) \cong A_4$.

5.53 证明 $\mathrm{PSL}(2,\mathbb{F}_9) \cong A_6$.

提示：设 $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ 和 $B = \begin{bmatrix} 1 & 1+u \\ 0 & 1 \end{bmatrix}$，其中 $u \in \mathbb{F}_9$ 满足 $u^2 = -1$. 如果 A 和 B 表示 $\mathrm{PSL}(2,\mathbb{F}_9)$ 中的元素 a 和 b，证明 ab 的阶为 5 且 $|\langle a,b \rangle| = 60$.

5.54 （i）证明 $\mathrm{SL}(2,\mathbb{F}_5)$ 不是可解群．

（ii）证明 $\mathrm{SL}(2,\mathbb{F}_5)$ 的一个西罗 2-子群同构于四元数群 $\mathbf{Q}$.

（iii）证明：如果 p 是奇素数，则 $\mathrm{SL}(2,\mathbb{F}_5)$ 的西罗 p-子群是循环群．由此推出，对每个整除 $|\mathrm{SL}(2,\mathbb{F}_5)|$ 的素数 p, $\mathrm{SL}(2,\mathbb{F}_5)$ 的一切西罗 p-子群有唯一的 p 阶子群．

5.55 证明 $\mathrm{GL}(2,\mathbb{F}_7)$ 不是可解群．

5.56 （i）证明对一切素数幂 $q \geqslant 4$, $\mathrm{SL}(2,\mathbb{F}_q)$ 是 $\mathrm{GL}(2,\mathbb{F}_q)$ 的换位子群．

（ii）当 $q=2$ 和 $q=3$ 时，$\mathrm{GL}(2,\mathbb{F}_q)$ 的换位子群是什么？ [296]

5.57 设 π 是 $\mathbb{F}_8$ 的本原元．

（i）$A = \begin{bmatrix} \pi & 0 \\ 1 & \pi \end{bmatrix}$ 作为 $\mathrm{GL}(2,\mathbb{F}_8)$ 的元素时，它的阶是多少？

（ii）$A = \begin{bmatrix} \pi & 0 & 0 \\ 1 & \pi & 0 \\ 0 & 1 & \pi \end{bmatrix}$ 作为 $\mathrm{GL}(3,\mathbb{F}_8)$ 的元素时，它的阶是多少？

提示：证明如果 $N=\begin{bmatrix}0&0&0\\1&0&0\\0&1&0\end{bmatrix}$，则 $N^2=\begin{bmatrix}0&0&0\\0&0&0\\1&0&0\end{bmatrix}$，$N^3=0$. 再用二项式定理证明 $A^m=\pi^m I+m\pi^{m-1}N+\binom{m}{2}\pi^{m-2}N^2$.

5.5 表现

怎样描述一个群？根据凯莱定理，有限群 G 同构于对称群 S_n 的子群，其中 $n=|G|$，从而群 G 恒可定义为由某种置换生成的 S_n 的子群．这种构造的一例出现在卡迈克尔（Carmichael）的群论书[⊖]中下面的练习中：

设 G 是由下面的置换生成的 S_{16} 的子群：

$$(a\,c)(b\,d);(e\,g)(f\,h);$$
$$(i\,k)(j\,\ell);(m\,o)(n\,p)$$
$$(a\,c)(e\,g)(i\,k);(a\,b)(c\,d)(m\,o);$$
$$(e\,f)(g\,h)(m\,n)(o\,p);(i\,j)(k\,\ell).$$

证明 $|G|=256$，$|G'|=16$，

$$\alpha=(i\,k)(j\,\ell)(m\,o)(n\,p)\in G',$$

但 α 不是换位子．

描述一个群的第二种方法是对某个 $n\geqslant 2$ 和某个域 k，用 $\mathrm{GL}(n,k)$ 代替 S_n[回忆一切 $n\times n$ 置换矩阵形成 $\mathrm{GL}(n,k)$ 的同构于 S_n 的子群，从而每个 n 阶群可以嵌入 $\mathrm{GL}(n,k)$]．我们已经用矩阵描述了几个群，例如，用这种方法定义了四元数群 $\mathbf{Q}$. 对于相对较小的群用置换或矩阵来描述是有效的，然而对于大的 n，这种描述是笨拙的．

也可以把群描述为由受制于某种关系的元素生成的，例如二面体群 D_{2n} 可以描述为这样的 $2n$ 阶群，它是由满足 $a^n=1=b^2$ 和 $bab=a^{-1}$ 的两个元素 a 和 b 生成的．考虑下面的定义．

297

定义 **广义四元数群 $\mathbf{Q}_n$**，其中 $n\geqslant 3$，是指由满足

$$a^{2^{n-1}}=1,bab^{-1}=a^{-1} \text{ 和 } b^2=a^{2^{n-2}}$$

的两个元素 a 和 b 生成的 2^n 阶群．

当 $n=3$ 时，就是 8 阶群 $\mathbf{Q}$. 该定义的一个显然的缺点是这种群的存在性留有疑问，例如 16 阶的这种群存在吗？注意，找到一个群 $G=\langle a,b\rangle$ 满足 $a^8=1$，$bab^{-1}=a^{-1}$ 和 $b^2=a^4$ 还是不够的．例如，有 $a^2=1$ 和 $b=1$ 的群 $G=\langle a,b\rangle$（当然，它是 2 阶循环群）就满足一切等式．

为了使这个描述变得严格，迪克（W. von Dyck）在 19 世纪 80 年代创造了**自由群**．

下面是自由群的现代定义．

定义 设 X 是群 F 的子集，如果对每个群 G 和每个函数 $f:X\to G$，存在唯一的同态 $\varphi:F\to G$ 使得对一切 $x\in X$，$\varphi(x)=f(x)$，

$$\begin{array}{ccc} F & & \\ \uparrow & \searrow^{\varphi} & \\ X & \xrightarrow{f} & G\end{array}$$

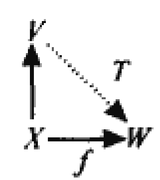
⊖ 卡迈克尔于 20 世纪 30 年代提出这个练习，在高速计算机时代之前，他能够手算出来．

则称 F 是以 X 为基的**自由群**.

这个定义模仿了线性代数中的一个基本结果，即定理 3.92，它是为什么可以用矩阵来描述线性变换的理由.

定理 设 $X = v_1,\cdots,v_n$ 是向量空间 V 的一个基. 如果 W 是一个向量空间且 $u_1,\cdots,u_n$ 是 W 中的一个表，则存在唯一的线性变换 $T: V \to W$ 使得对一切 $i, T(v_i) = u_i$.

我们注意到给定 W 中的向量表 $u_1,\cdots,u_n$ 和给定满足 $f(v_i) = u_i$ 的函数 $f: X \to W$ 是同一件事，由此我们可画出上面这个定理的图，毕竟一个函数 $f: X \to W$ 由它在 $v_i \in X$ 上的值所确定.



如果知道自由群是存在的，则可以如下定义 $\mathbf{Q}_n$. 设 F 是以 $X = \{x,y\}$ 为基的自由群，R 是由 $\{x^{2^{n-1}}, yxy^{-1}x, y^{-2}x^{2^{n-2}}\}$ 生成的 F 的正规子群，定义 $\mathbf{Q}_n = F/R$. 显然 F/R 是由两个元素 $a = xR$ 和 $b = yR$ 生成的群，它满足定义中的关系，不清楚的是 F/R 的阶为 2^n，这是需要证明的（见命题 5.80）. 298

第一个问题是自由群是否存在. 这个构造的思想是简单而自然的，但详细验证有点繁琐. 我们先来描述自由群的成分.

设 X 是一个非空集合，并设 X^{-1} 是 X 的不相交的复制，即 X 和 X^{-1} 不相交且存在双射 $X \to X^{-1}$，记为 $x \mapsto x^{-1}$. 定义 X 上的**字母表**为

$$X \cup X^{-1}.$$

如果 n 是正整数，定义 X 上的**长度**为 $n \geqslant 1$ 的**字**是函数 $w: \{1,2,\cdots,n\} \to X \cup X^{-1}$. 习惯上，我们记长度 n 的字 w 如下：如果 $w(i) = x_i^{e_i}$，则

$$w = x_1^{e_1} \cdots x_n^{e_n},$$

其中 $x_i \in X, e_i = \pm 1$. 字 w 的长度 n 记为 $|w|$. 例如 $|xx^{-1}| = 2$. **空字**记为 1，是一个新符号，空字的长度定义为 0.

函数相等的定义在这里是如下的意义. 如果 $u = x_1^{e_1} \cdots x_n^{e_n}$ 和 $v = y_1^{d_1} \cdots y_m^{d_m}$ 都是字，其中对一切 i,j 有 $x_i, y_j \in X$，则 $u = v$ 当且仅当 $m = n$ 且对一切 $i, x_i = y_i, e_i = d_i$；于是每个字的拼写法唯一.

定义 字 $w = x_1^{e_1} \cdots x_n^{e_n}$ 的**子字**不是空字就是形如 $u = x_r^{e_r} \cdots x_s^{e_s}$ 的字，其中 $1 \leqslant r \leqslant s \leqslant n$. 字 $w = x_1^{e_1} \cdots x_n^{e_n}$ 的**逆**是 $w^{-1} = x_n^{-e_n} \cdots x_1^{-e_1}$.

由此对每个字 $w, (w^{-1})^{-1} = w$.

最重要的字是既约字.

定义 X 上的字称为**既约的**，如果 $w = 1$ 或 w 没有形如 xx^{-1} 或 $x^{-1}x$ 的子字，其中 $x \in X$.

X 上的任意两个字可以相乘.

定义 如果 $u = x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ 和 $v = y_1^{d_1} \cdots y_m^{d_m}$ 是 X 上的字，则它们的**并置**是指字

$$uv = x_1^{e_1} \cdots x_n^{e_n} y_1^{d_1} \cdots y_m^{d_m}.$$

如果 1 是空字，则 $1v = v$ 和 $u1 = u$.

我们尝试定义自由群为 X 上的一切字的集合，它的运算为并置，幺元为空字 1，$w = x_1^{e_1} \cdots x_n^{e_n}$ 的逆为 $w^{-1} = x_n^{-e_n} \cdots x_1^{-e_1}$. 有一个问题：如果 $x \in X$，则我们要求 $x^{-1}x = 1$，而这是不能成立的，

$x^{-1}x$ 的长度为 2，不是 0. 我们可以尝试限制 F 的元素为 X 上的既约字以弥补这个缺陷，但是即使 u 和 v 都是既约的，它们的并置 uv 也未必是既约的．当然，可以用消去的方法把 uv 改变为既约字，但此时证明结合性是棘手的．我们解决这个问题如下．举例来说，因为像 $zx^{-1}xyzx^{-1}$ 和 $zyzx^{-1}$ 这样的字必须恒等，所以利用 X 上一切字的集合上的一个等价关系是有道理的．如果定义 F 的元素为等价类，则结合性的证明不会很困难，且在每个等价类中有唯一的既约字．所以可以把 F 的元素看作既约字，而把两个元素的乘积看作是它们并置后再约化㊀.

299

不经意的读者可以像刚才描述的那样接受自由群的存在性，从而跳过下面一段到命题 5.73. 下面是对其他那些读者的详细论证．

定义 设 A 和 B 是 X 上的字，可以是空字，并设 $w=AB$. 一个**初等运算**是指一个**插入**，它把 $w=AB$ 变成 $Aaa^{-1}B$，其中 $a\in X\cup X^{-1}$，或者是把 w 的形如 aa^{-1} 的子字**消去**，它把 $w=Aaa^{-1}B$ 变成 AB.

定义 用

$$w\to w'$$

表示 w 经一个初等运算得到 w'. 对于 X 上的两个字 u 和 v，如果存在字 $u=w_1,w_2,\cdots,w_n=v$ 和初等运算

$$u=w_1\to w_2\to\cdots\to w_n=v,$$

则称 u 和 v **等价**，记为 $u\sim v$. 记字 w 的等价类为$[w]$.

注意 $xx^{-1}\sim 1$ 和 $x^{-1}x\sim 1$，即 $[xx^{-1}]=[1]=[x^{-1}x]$.

我们分两步构造自由群．

定义 **半群**是指有结合运算的集合；**幺半群**是指有幺元 1 的半群 S，即对一切 $s\in S, 1s=s=s1$. 如果 S 和 S' 是半群，则称满足 $f(xy)=f(x)f(y)$ 的函数 $f:S\to S'$ 为**同态**. 如果 S 和 S' 是幺半群，则**同态** $f:S\to S'$ 必须满足 $f(1)=1$.

当然，每个群都是幺半群，群之间的同态是它们作为幺半群的同态．

例 5.69 （ⅰ）自然数N 的集合是加法下的交换幺半群．

（ⅱ）幺半群的直积也是幺半群（运算为坐标状态的运算）．特别是自然数的一切 n 元组的集合 $\mathbb{N}^n$ 是加法交换幺半群． ■

下面是非交换幺半群的例子．

引理 5.70 设 X 是集合，并设 $\mathcal{W}(X)$ 是 X 上一切字的集合［如果 $X=\varnothing$，则 $\mathcal{W}(X)$ 只由一个空字组成］．

300

（ⅰ）$\mathcal{W}(X)$ 在并置运算下是幺半群．

（ⅱ）如果 $u\sim u'$ 和 $v\sim v'$，则 $uv\sim u'v'$.

（ⅲ）如果 G 是群，$f:X\to G$ 是函数，则存在扩张 f 的同态 $\tilde{f}:\mathcal{W}(X)\to G$ 使得 $w\sim w'$ 蕴涵 G 中的 $\tilde{f}(w)=\tilde{f}(w')$.

证明 （ⅰ）一旦注意到 $\mathcal{W}(X)$ 中没有消去发生，并置的结合性就显而易见．

（ⅱ）若干初等运算把 u 变到 u'，当应用到字 uv 上时，得到一个链把 uv 变到 $u'v$. 若干初等运

㊀ 在集合 X 上构造阿贝尔群的另一种方法是使用范德瓦尔登（van der Waerden）技巧：设 Ω 是 X 上所有约化字的集合，证明对称群 S_Ω 的某个子群是以 X 为基的自由群．(见罗特曼所著的《An Introduction to the Theory of Groups》344～345 页.)

算把 v 变到 v'，当应用到字 $u'v$ 时，得到一个链把 $u'v$ 变到 $u'v'$. 因此 $uv \sim u'v'$.

（iii）如果 $w = x_1^{e_1} \cdots x_n^{e_n}$，则定义

$$\tilde{f}(w) = f(x_1)^{e_1} f(x_2)^{e_2} \cdots f(x_n)^{e_n}.$$

w 的拼写法唯一说明 $\tilde{f}$ 是合理定义的函数，显然 $\tilde{f}: \mathcal{W}(X) \to G$ 是同态.

设 $w \sim w'$，我们对从 w 变到 w' 的链中初等运算的个数用归纳法证明 G 中有 $\tilde{f}(w) = \tilde{f}(w')$. 考虑消去 $w = Aaa^{-1}B \to AB$，其中 A 和 B 都是 w 的子字. $\tilde{f}$ 是同态给出

$$\tilde{f}(Aaa^{-1}B) = \tilde{f}(A)\tilde{f}(a)\tilde{f}(a)^{-1}\tilde{f}(B).$$

但在群 G 中有消去，所以在 G 中

$$\tilde{f}(A)\tilde{f}(a)\tilde{f}(a)^{-1}\tilde{f}(B) = \tilde{f}(A)\tilde{f}(B),$$

从而 $\tilde{f}(Aaa^{-1}B) = \tilde{f}(AB)$. 对于插入可类似地论证. ■

下一命题用来证明自由群中的每个元素都有一个范式.

命题 5.71 集合 X 上的每个字等价于唯一的一个既约字.

证明 如果 $X = \varnothing$，则 X 上只有一个字，就是空字 1，1 是既约的.

如果 $X \neq \varnothing$，我们先证明存在既约字等价于 w. 如果 w 没有形如 aa^{-1} 的子字，其中 $a \in X \cup X^{-1}$，则 w 是既约的. 否则，消去第一个这样的对产生一个新字 w_1 满足 $|w_1| < |w|$，它可能是空字. 现在重复下述过程：如果 w_1 是既约的，停止；如果 w_1 存在形如 aa^{-1} 的子字，则消去它，产生更短的字 w_2. 因长度严格递减，该过程终止于一个既约字，它和 w 等价.

为证明唯一性，假设存在不同的既约字 u 和 v 以及初等运算的链

$$u = w_1 \to w_2 \to \cdots \to w_n = v;$$

可以假定 n 是极小的. 因 u 和 v 都是既约的，第一个初等运算必是插入，而最后一个初等运算必是消去，因此必有第一个消去，比如 $w_i \to w_{i+1}$. 于是，初等运算 $w_{i-1} \to w_i$ 插入 aa^{-1}，而初等运算 $w_i \to w_{i+1}$ 消去 bb^{-1}，其中 $a, b \in X \cup X^{-1}$. [301]

有三种情形. 如果 w_i 的子字 aa^{-1} 和 bb^{-1} 相同，则 $w_{i-1} = w_{i+1}$，因为 w_{i+1} 是从 w_{i-1} 先插入 aa^{-1} 再消去它得到的，由此链

$$u = w_1 \to w_2 \to \cdots \to w_{i-1} = w_{i+1} \to \cdots \to w_n = v$$

比原始的最短链还短. 第二种情形，w_i 的子字 aa^{-1} 和 bb^{-1} 重叠，出现这种情形有两种方式，一种方式是

$$w_i = Aaa^{-1}b^{-1}C,$$

其中 A, C 是 w_i 的子字，且 $a^{-1} = b$；因此 $a = b^{-1}$，且

$$w_i = Aaa^{-1}aC.$$

因为插入 aa^{-1}，所以 $w_{i-1} = AaC$. 又因为消去 $bb^{-1} = a^{-1}a$，所以 $w_{i+1} = AaC$. 于是 $w_{i-1} = w_{i+1}$，移去 w_i 得到较短的链. 重叠出现的第二种方式是 $w_i = Aa^{-1}aa^{-1}C$，其中 $b^{-1} = a$，和第一种方式一样导出 $w_{i-1} = w_{i+1}$.

最后，假设子字 aa^{-1} 和 bb^{-1} 不重叠：

$$w_i = A'aa^{-1}A''bb^{-1}C, w_{i+1} = A'aa^{-1}A''C.$$

现在 bb^{-1} 成为 w_i 的子字，这由先前把 bb^{-1} 或 $b^{-1}b$ 插入某个字 $w_{j-1} = XY$（其中 $j < i$）来实现；即 $w_{j-1} \to w_j$，其中 $w_j = Xbb^{-1}Y$ 或 $w_j = Xb^{-1}bY$. 在第一种场合中，子链 $w_{j-1} \to \cdots \to w_{i+1}$ 有如

$$XY \to Xbb^{-1}Y \to \cdots \to Abb^{-1}C \to A'aa^{-1}A''bb^{-1}C \to A'aa^{-1}A''C,$$

其中 $A=A'A''$. 但我们可以不插入 bb^{-1} 从而缩短这个链：

$$XY \to \cdots \to AC \to A'aa^{-1}A''C.$$

在第二种场合中，要使 bb^{-1} 的消去能够发生，只能是在 $w_{j-1}=XY$ 中有 $X=X'b$ 或 $Y=b^{-1}Y'$. 如果 $X=X'b$，则 $w_{j-1}=X'bY$ 且 $w_j=X'bb^{-1}bY$（子字 bb^{-1} 就是要被初等运算 $w_i \to w_{i+1}$ 消去的字）. 和第一种可能性一样，我们不需要插入. 更详细地说，链

$$X'bY \to X'bb^{-1}bY \to \cdots \to Abb^{-1}C \to A'aa^{-1}A''bb^{-1}C \to A'aa^{-1}A''C$$

（其中过程 $X' \to A$ 和 $bY \to C$ 只涉及插入）可以移去 $b^{-1}b$ 的插入而缩短：

$$X'bY \to \cdots \to AC \to A'aa^{-1}A''C.$$

第二种情形，$Y=b^{-1}Y'$ 可以同样处理. 因此在所有情形中，我们都可以缩短最短的链，从而这样的链不存在. ■

302

定理 5.72 如果 X 是集合，则 X 上字的一切等价类的集合 F 连同运算 $[u][v]=[uv]$ 是以 $\{[x]: x \in X\}$ 为基的自由群.

此外，F 中的每个元素都有范式：对每个 $[u] \in F$，存在既约字 w 使得 $[u]=[w]$.

证明 如果 $X=\varnothing$，则 $\mathcal{W}(\varnothing)$ 只由一个空字组成，从而 $F=\{1\}$，读者可以证明这确实是 $\varnothing$ 上的自由群.

现在假定 $X \neq \varnothing$. 在引理5.7(ii)中已经看到并置与等价关系相容，从而 F 上的运算是合理定义的. 由于 $\mathcal{W}(X)$ 中的结合性：

$$\begin{aligned}[u]([v][w]) &= [u][vw] \\ &= [u(vw)] \\ &= [(uv)w] \\ &= [uv][w] \\ &= ([u][v])[w],\end{aligned}$$

这个运算是结合的. 幺元是类 $[1]$，$[w]$ 的逆是 $[w^{-1}]$，从而 F 是群.

如果 $[w] \in F$，则

$$[w]=[x_1^{e_1}\cdots x_n^{e_n}]=[x_1^{e_1}][x_2^{e_2}]\cdots[x_n^{e_n}],$$

其中对一切 i，$e_i=\pm 1$，因此 F 由 X 生成（如果把每个 $x \in X$ 等同于 $[x]$）. 根据命题 5.71，对每个 $[w]$，存在唯一的一个既约字 u 使得 $[w]=[u]$.

为证明 F 是自由的且具有基 X，假设 $f: X \to G$ 是函数，其中 G 是群. 定义 $\varphi: F \to G$ 为

$$\varphi: [x_1^{e_1}][x_2^{e_2}]\cdots[x_n^{e_n}] \mapsto f(x_1)^{e_1} f(x_2)^{e_2}\cdots f(x_n)^{e_n},$$

其中 $x_1^{e_1}\cdots x_n^{e_n}$ 是既约的. 字的既约表达式的唯一性表明 φ 是合理定义的函数（它显然是 f 的扩张）. 注意到引理 5.70 中 φ 和同态 $\tilde{f}: \mathcal{W}(X) \to G$ 之间的关系：当 w 是既约字时，

$$\varphi([w])=\tilde{f}(w).$$

剩下的是证明 φ 是同态（如果是同态，它就是扩张 f 的唯一同态，因为子集 X 生成 F）. 设 $[u],[v] \in F$，其中 u,v 是既约字，并设 $uv \sim w$，其中 w 也是既约字. 现在因为 w 是既约字，所以

$$\varphi([u])[v])=\varphi([w])=\tilde{f}(w),$$

又因为 u，v 是既约字，所以

$$\varphi([u])\varphi([v]) = \tilde{f}(u)\,\tilde{f}(v).$$

最后，由引理5.70(ⅲ)，$\tilde{f}(u)\,\tilde{f}(v) = \tilde{f}(w)$. 因此 $\varphi([u][v]) = \varphi([u])\varphi([v])$. ■

303

注 对于以给定集合 X 为基的自由群 F 的存在性，有一个不太繁琐的证明，它属于 M. Barr（见 Montgomery-Ralston，《Selected Papers in Algebra》）. 这里没有给出这个证明，因为它没有描述 F 的元素，而这个描述在用到自由群时常常是需要的.

我们已经证明对每个集合 X，存在以 X 为基的自由群. 此外，X 上的自由群 F 的元素可以看作既约字，而运算可以看作并置再约化. 括号不再使用，F 的元素 $[w]$ 写作 w.

我们刚刚构造的以 X 为基的自由群 F 是由 X 生成的. 基是同一 X 的两个自由群同构吗?

命题 5.73 （ⅰ）设 X_1 是自由群 F_1 的基，X_2 是自由群 F_2 的基. 如果存在双射 $f: X_1 \to X_2$，则存在扩张 f 的同构 $\varphi: F_1 \to F_2$.

（ⅱ）如果 F 是基为 X 的自由群，则 F 由 X 生成.

证明 （ⅰ）下面的图将帮助读者理解证明，其中垂直箭头是包含函数.

$$\begin{array}{ccc} F_1 & \underset{\varphi_2}{\overset{\varphi_1}{\rightleftarrows}} & F_2 \\ \uparrow & & \uparrow \\ X_1 & \underset{f^{-1}}{\overset{f}{\rightleftarrows}} & X_2. \end{array}$$

因为 $X_2 \subseteq F_2$，我们可以把 f 的目标域看作 F_2. 因 F_1 是以 X_1 为基的自由群，所以存在同态 $\varphi_1: F_1 \to F_2$ 扩张 f. 同样，存在同态 $\varphi_2: F_2 \to F_1$ 扩张 f^{-1}. 因此复合 $\varphi_2\varphi_1: F_1 \to F_1$ 是扩张 1_X 的同态. 而恒等函数 1_{F_1} 也扩张 1_X，从而扩张的唯一性给出 $\varphi_2\varphi_1 = 1_{F_1}$. 用同样的方法可以知道另一个复合 $\varphi_1\varphi_2 = 1_{F_2}$，所以 φ_1 是同构.

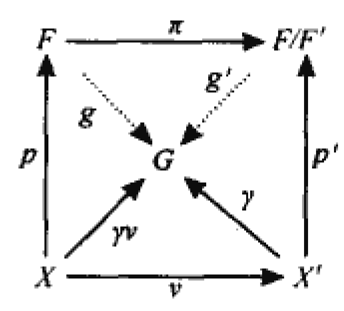
（ⅱ）设对于某个集合 X_1，存在双射 $f: X_1 \to X$. 如果 F_1 是定理5.72中构造出来的以 X_1 为基的自由群，则 X_1 生成 F_1. 根据（ⅰ），存在同构 $\varphi: F_1 \to F$ 使得 $\varphi(X_1) = X$. 而如果 X_1 生成 F_1，则 $\varphi(X_1)$ 生成 $\mathrm{im}\varphi$，即 X 生成 F. ■

自由群有秩的概念，但我们必须首先验证一个自由群中的一切基所含元素的个数相同.

引理 5.74 如果 F 是以 $X = x_1, \cdots, x_n$ 为基的自由群，则 F/F' 是以 $X' = x_1F', \cdots, x_nF'$ 为基的自由阿贝尔群，其中 F' 是 F 的换位子群.

304

证明 首先注意到 X' 生成 F/F'，这是根据命题5.73(ⅱ)，它说 X 生成 F. 我们用命题5.12中的准则证明 F/F' 是以 X' 为基的自由阿贝尔群. 考虑下面的图.



这里 G 是任意阿贝尔群，p 和 p' 是包含函数，π 是自然映射，$\nu: x \mapsto xF'$，$\gamma: X' \to G$ 是函数. 令 $g: F \to G$ 是自由群的定义给出的满足 $gp = \gamma\nu$ 的唯一同态(因 $\gamma\nu: X \to G$ 是函数)，定义 $g': F/F' \to G$ 为 $wF' \mapsto g(w)$（g' 是合理定义的，因为 G 是阿贝尔群迫使 $F' \leqslant \ker g$）. 现在因为

$$g'p'\nu = g'\pi p = gp = \gamma\nu$$

且 ν 是满射，所以 $g'p'=\gamma$. 最后，g' 是满足 $g'p'=\gamma$ 的唯一映射，这是因为如果 $g''p'=\gamma$，则 g' 和 g'' 在生成集 X' 上一致，因此相等. ■

命题 5.75 设 F 是以 X 为基的自由群. 如果 $|X|=n$，则 F 的每个基都有 n 个元素.

证明 根据引理，F/F' 是秩为 n 的自由阿贝尔群. 另一方面，如果 $y_1,\cdots,y_m$ 是 F 的另一组基，则 F/F' 是秩为 m 的自由阿贝尔群，根据命题 5.9，有 $m=n$. ■

下面的定义现在有意义了.

定义 自由群 F 的**秩**是指一组基中元素的个数，记为 $\text{rank}(F)$.

命题5.73(ⅰ)现在可以重新陈述为：秩有限的两个自由群同构当且仅当它们有相同的秩.

命题 5.76 每个群 G 都是一个自由群的商群.

证明 设 X 是存在双射 $f: X\to G$ 的一个集合(例如，可取 X 为 G 的底集和 $f=1_G$)，并设 F 是以 X 为基的自由群，存在扩张 f 的同态 $\varphi: F\to G$,因为 f 是满射，所以 φ 也是满射. 因此 $G\cong F/\ker\varphi$. ■

305

我们回到群的描述.

定义 群 G 的**表现**是指有序对

$$G=(X\mid R),$$

其中 X 是集合，R 是 X 上字的一个集合，且 $G=F/N$，其中 F 是以 X 为基的自由群，N 是 R **生成的正规子群**；即 R 中元素的一切共轭生成的子群. 我们称集合 X 为**生成元**[㊀]，集合 R 为**关系**.

命题 5.76 说每个群都有表现.

定义 如果群 G 有一个表现 $(X\mid R)$，其中 X 是有限集，则称群 G 是**有限生成**的. 如果群 G 有一个表现 $(X\mid R)$，其中 X 和 R 都是有限的，则称群 G 是**有限表现**的.

易知群 G 是有限生成的当且仅当存在有限集 $A\subseteq G$ 使得 $G=\langle A\rangle$. 确实存在不是有限表现的有限生成群（见《An Introduction to the Theory of Groups》[㊁]417 页）.

注 群论和代数拓扑之间存在重要的联系. 如果 X 是一个拓扑空间，则它的基本群 $\pi_1(X)$ 定义为连续函数 $S^1\to X$ 的一切同伦类的集合，其中 S^1 是单位圆. 一个有限单纯复形是一个可剖分的拓扑空间，所谓可剖分是指这个空间是有限个顶点，边，三角形，四面体等的并. 我们可以证明一个群 G 是有限表现的当且仅当存在有限单纯复形 X 使得 $G\cong\pi_1(X)$. 对于一个群，经常只知道它的某个表现. 例如，假设 X 是一个单纯复形，它包含子复形 Y_1 和 Y_2 满足 $Y_1\cup Y_2=X$ 和 $Y_1\cap Y_2$ 是连通的，则**范坎彭**（van Kampen）定理说，如果知道 $\pi_1(Y_1)$ 和 $\pi_1(Y_2)$ 的表现就可以给出 $\pi_1(X)$ 的表现.

例 5.77 （ⅰ）一个群有许多表现. 例如，$G=\mathbb{I}_6$ 有表现

$$(x\mid x^6)$$

和

$$(a,b\mid a^3,b^2,aba^{-1}b^{-1}).$$

一个基本问题是如何确定两个表现是否给出同构群. 可以证明不存在解该问题的算法（见罗特曼所著的《An Introduction to the Theory of Groups》，469 页）.

（ⅱ）以 X 为基的自由群有表现

$$(X\mid\varnothing).$$

㊀ 这里的术语生成元是广义用法，因为 X 不是 G 的子集. 在通常意义下，$G=F/N$ 的子集 $\{xN: x\in X\}$ 才生成 G.

㊁ 该书是本书作者所著的另一本书. ——编辑注

自由群所以有这个准确的名称正因为它有无关系的表现． ■ [306]

关于记号说一句话．我们时常把表现中的关系写作等式．于是I_6第二个表现中的关系

$$a^3, b^2, aba^{-1}b^{-1}$$

可以写作

$$a^3 = 1, b^2 = 1, ab = ba.$$

如果r是$x_1, \cdots, x_n$上的字，可以记$r = r(x_1, \cdots, x_n)$．如果H是群且$h_1, \cdots, h_n \in H$，则$r(h_1, \cdots, h_n)$表示在r中把每个x_i换成h_i得到的H中的元素．

下一个基本结果十分有用，我们只叙述它是有限生成的情形．

定理 5.78（von Dyck 定理） *设群G有表现*

$$G = (x_1, \cdots, x_n \mid r_j, j \in J);$$

即$G = F/N$，其中F是$\{x_1, \cdots, x_n\}$上的自由群，N是由一切$r_j = r_j(x_1, \cdots, x_n)$生成的$F$的正规子群．如果$H = \langle h_1, \cdots, h_n \rangle$是群且在$H$中对一切$j \in J$有$r_j(h_1, \cdots, h_n) = 1$，则对一切$i$存在满足$x_iN \mapsto h_i$的满同态$G \to H$.

证明 如果F是以$\{x_1, \cdots, x_n\}$为基的自由群，则存在同态$\varphi: F \to H$使得对一切i有$\varphi(x_i) = h_i$．因在H中对一切$j \in J$有$r_j(h_1, \cdots, h_n) = 1$，从而对一切$j \in J$有$r_j \in \ker\varphi$，由此$N \leqslant \ker\varphi$．所以$\varphi$导出一个（合理定义的）同态$G = F/N \to H$，它对一切$i$满足$x_iN \mapsto h_i$. ■

下一命题将表明 von Dyck 定理如何分析表现，但我们先构造一个具体的矩阵群．

例 5.79 我们要构造一个群H_n，它是 298 页定义的广义四元数群$\mathbf{Q}_n$的一个好的候选者，其中$n \geqslant 3$．考虑复数矩阵

$$A = \begin{bmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{bmatrix} \text{和} B = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix},$$

其中ω是2^{n-1}次单位原根，并设$H_n = \langle A, B \rangle \leqslant \mathrm{GL}(2, \mathbb{C})$．我们断言$A$和$B$满足广义四元数群定义中的关系．对一切$i \geqslant 1$，

$$A^{2^i} = \begin{bmatrix} \omega^{2^i} & 0 \\ 0 & \omega^{-2^i} \end{bmatrix},$$

从而$A^{2^{n-1}} = I$；事实上，A的阶为2^{n-1}．此外，

$$B^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = A^{2^{n-2}}, \qquad BAB^{-1} = \begin{bmatrix} \omega^{-1} & 0 \\ 0 & \omega \end{bmatrix} = A^{-1}.$$

[307]

注意，A和B不交换，因此$B \notin \langle A \rangle$，从而陪集$\langle A \rangle$和$B\langle A \rangle$不同．因$A$的阶为$2^{n-1}$，从而导出

$$|H_n| \geqslant |\langle A \rangle \cup B\langle A \rangle| = 2^{n-1} + 2^{n-1} = 2^n.$$

下一定理将证明$|H_n| = 2^n$. ■

命题 5.80 *对每个$n \geqslant 3$，存在广义四元数群$\mathbf{Q}_n$.*

证明 设G_n是由表现

$$G_n = (a, b \mid a^{2^{n-1}} = 1, bab^{-1} = a^{-1}, b^2 = a^{2^{n-2}})$$

定义的群．群G_n满足广义四元数群定义中的一切要求，只有一个可能的例外：我们尚不知道它的阶是2^n．根据 von Dyck 定理，存在满同态$G_n \to H_n$，其中H_n是刚在例 5.79 中构造的群．因此

$|G_n| \geqslant 2^n$.

另一方面，G_n 中的循环子群 $\langle a \rangle$ 的阶最多为 2^{n-1}，这是因为 $a^{2^{n-1}}=1$. 关系 $bab^{-1}=a^{-1}$ 蕴涵 $\langle a \rangle \lhd G_n = \langle a,b \rangle$，从而 $G_n/\langle a \rangle$ 是由 b 的象生成的．最后，关系 $b^2=a^{2^{n-2}}$ 表明 $|G_n/\langle a \rangle| \leqslant 2$. 因此

$$|G_n| \leqslant |\langle a \rangle| \, |G_n/\langle a \rangle| \leqslant 2^{n-1} \cdot 2 = 2^n.$$

所以 $|G_n| = 2^n$，从而 $G_n \cong \mathbf{Q}_n$. ■

现在可知例 5.79 中的群 H_n 同构于 $\mathbf{Q}_n$.

在习题 2.57 中给出了二面体群 D_{2n} 的一个具体构造，我们可以用刚才证明中给出的那种群得到这个群的一个表现．

命题 5.81 *二面体群 D_{2n} 有表现*

$$D_{2n} = (a,b \mid a^n = 1, b^2 = 1, bab = a^{-1}).$$

证明 令 C_{2n} 表示命题中的表现定义的群，并令 D_{2n} 是习题 2.57 中构造的 $2n$ 阶群．根据 von Dyck 定理，存在满同态 $f: C_{2n} \to D_{2n}$，从而 $|C_{2n}| \geqslant 2n$．为证明 f 是同构，我们证明反过来的不等式．C_{2n} 中的循环子群 $\langle a \rangle$ 的阶最多为 n，这是因为 $a^n=1$. 关系 $bab^{-1}=a^{-1}$ 蕴涵 $\langle a \rangle \lhd C_{2n} = \langle a,b \rangle$，从而 $C_{2n}/\langle a \rangle$ 是由 b 的象生成的．最后，关系 $b^2=1$ 表明 $|C_{2n}/\langle a \rangle| \leqslant 2$. 因此

$$|C_{2n}| \leqslant |\langle a \rangle| \, |C_{2n}/\langle a \rangle| \leqslant 2n.$$

所以 $|C_{2n}| = 2n$，从而 $C_{2n} \cong D_{2n}$. ■

在第 2 章中，我们对 7 阶或小于 7 阶的群进行了分类．因素数阶群都是循环群，所以只有 4 阶群和 6 阶群的分类有问题．命题 2.90 中给出的每个 6 阶非阿贝尔群同构于 S_3 的证明相当复杂，它分析了群在一个循环子群的陪集上的表示．下面是在现在水平上的一个证明．

308

命题 5.82 *如果 G 是 6 阶非阿贝尔群，则 $G \cong S_3$.*

证明 和命题 2.90 的证明一样，G 必包含 3 阶元素 a 和 2 阶元素 b. 现在因为 $\langle a \rangle$ 的指数为 2，所以 $\langle a \rangle \lhd G$，从而或者 $bab^{-1}=a$，或者 $bab^{-1}=a^{-1}$. 因为 G 不是阿贝尔群，第一种情形不可能发生．所以 G 满足 $D_6 \cong S_3$ 的表现中的条件，于是 von Dyck 定理给出满同态 $D_6 \to G$. 因两个群的阶相同，这个映射必是同构． ■

我们现在对 8 阶群进行分类．

定理 5.83 *每个 8 阶群同构于*

$$D_8, \mathbf{Q}, \mathbb{I}_8, \mathbb{I}_4 \oplus \mathbb{I}_2 \text{ 或 } \mathbb{I}_2 \oplus \mathbb{I}_2 \oplus \mathbb{I}_2.$$

此外，列出的任两个群不同构．

证明 如果 G 是阿贝尔群，则基定理表明 G 是循环群的直和，而基本定理证明这种群只有列出的那几种．所以可以假定 G 不是阿贝尔群．

现在 G 不可能有 8 阶元素，否则它就是循环群，因此是阿贝尔群．此外每个非幺元元素的阶不为 2，否则根据习题 2.26，G 是阿贝尔群．由此可知，G 必有一个 4 阶元素 a，因此 $\langle a \rangle$ 的指数为 2，从而 $\langle a \rangle \lhd G$. 选取 $b \in G$ 满足 $b \notin \langle a \rangle$. 注意，因为 $\langle a \rangle$ 的指数为 2，因此它必是一个极大子群，从而 $G = \langle a,b \rangle$. 现在由于 $G/\langle a \rangle$ 是 2 阶群，所以 $b^2 \in \langle a \rangle$，从而 $b^2=a^i$，其中 $0 \leqslant i \leqslant 3$. 不可能有 $b^2=a$ 或 $b^2=a^3=a^{-1}$，否则 b 的阶为 8. 所以

$$b^2 = a^2 \quad \text{或} \quad b^2 = 1.$$

此外，由正规性，$bab^{-1} \in \langle a \rangle$，从而 $bab^{-1}=a$ 或 $bab^{-1}=a^{-1}$（因为 bab^{-1} 和 a 有相同的阶）．现在

$bab^{-1}=a$ 说明 a 和 b 可交换，这蕴涵 G 是阿贝尔群．由此可知 $bab^{-1}=a^{-1}$．所以只有两种可能性：

$$a^4=1, b^2=a^2, bab^{-1}=a^{-1}$$

或

$$a^4=1, b^2=1, bab^{-1}=a^{-1}.$$

根据引理，第一组等式给出 $\mathbf{Q}$ 的表现中的关系，而命题 5.81 表明第二组等式给出 D_8 的表现中的关系．根据 von Dyck 定理，存在满同态 $\mathbf{Q}\to G$ 或 $D_8\to G$. 然而 $|G|=8$，这个同态必是同构．

最后，习题 2.61 证明 $\mathbf{Q}$ 和 D_8 不同构（例如，$\mathbf{Q}$ 的 2 阶元素唯一，而 D_8 有好几个 2 阶元素）．∎

读者可以对小阶群 G 继续进行分类，比方说，$|G|\leqslant 15$. 这里是分类的结果．根据系 2.104，每个 p^2 阶群是阿贝尔群，其中 p 是素数，所以每个 9 阶群是阿贝尔群，根据有限群的基本定理，只有两个这样的群：$\mathbb{I}_9$ 和 $\mathbb{I}_3\times\mathbb{I}_3$. 如果 p 是素数，则每个 $2p$ 阶群或者是循环群，或者是二面体群（见习题 5.63）．于是 10 阶群只有两个，14 阶群也只有两个．12 阶群有 5 个，其中两个是阿贝尔群，12 阶非阿贝尔群是 $D_{12}\cong S_3\times\mathbb{I}_2, A_4$ 和一个表现为 [309]

$$T=(a,b \mid a^6=1, b^2=a^3=(ab)^2)$$

的群 T；见习题 5.64，该题中把 T 理解为一个矩阵群．群[⊖] T 是半直积的例子，这种构造将在第 10 章中讨论．如果 $p<q$ 都是素数且 $q\not\equiv 1 \bmod p$，则 pq 阶群必是循环群，因此 15 阶群只有一个［见习题10.11(ii)］．有 14 个不同构的 16 阶群，因而在这里停止是恰当的．

习题

5.58　设 F 是以 X 为基的自由群且 $A\subseteq X$. 证明：如果 N 是由 A 生成的 F 的正规子群，则 F/N 是自由群．

5.59　设 F 是自由群．

(i) 证明 F 没有有限阶元素（除 1 外）．

(ii) 证明自由群 F 是阿贝尔群当且仅当 $\text{rank}(F)\leqslant 1$.

提示：把秩 $\geqslant 2$ 的自由群映射到一个非阿贝尔群上．

(iii) 证明：如果 $\text{rank}(F)\geqslant 2$，则 $Z(F)=\{1\}$，其中 $Z(F)$ 是 F 的中心．

5.60　证明自由群是可解的当且仅当它是无限循环群（见 286 页）．

5.61　(i) 如果 G 是有限生成群且 n 是正整数，证明 G 只有有限个指数为 n 的子群．

提示：考虑同态 $G\to S_n$.

(ii) 设 H 和 K 是群 G 中指数有限的子群，证明 $H\cap K$ 也是 G 中指数有限的子群．

5.62　(i) 证明每个广义四元数群 $\mathbf{Q}_n$ 有唯一的 2 阶子群，就是 $\langle b^2\rangle$，且这个子群是中心 $Z(\mathbf{Q}_n)$.

(ii) 证明 $\mathbf{Q}_n/Z(\mathbf{Q}_n)\cong D_{2^{n-1}}$.

5.63　如果 p 是素数，证明每个 $2p$ 阶群或者是循环群，或者同构于 D_{2p}.

提示：根据柯西定理，G 必包含一个 p 阶元素 a，因为 $\langle a\rangle$ 的指数为 2，所以 $\langle a\rangle\lhd G$.

5.64　设 G 是由

$$\begin{bmatrix}\omega & 0\\ 0 & \omega^2\end{bmatrix} \text{和} \begin{bmatrix}0 & \mathrm{i}\\ \mathrm{i} & 0\end{bmatrix}$$

生成的 $\mathrm{GL}(2,\mathbb{C})$ 的子群，其中 $\omega=e^{2\pi i/3}$ 是三次单位原根．

⊖ 在 Coxeter 和 Moser 所著的《Generators and Relations for Discrete Groups》中，把群 T 叫做（2，2，3）型双循环群．但这个术语没有被广泛接受．

310

(i) 证明 G 是不同构于 A_4 也不同构于 D_{12} 的 12 阶群.

(ii) 证明 G 同构于 310 页上的群 T.

5.65 证明每个有限群都是有限表现群.

5.66 计算具有表现

$$G=(a,b,c,d \mid bab^{-1}=a^2, bdb^{-1}=d^2, c^{-1}ac=b^2, dcd^{-1}=c^2, bd=db)$$

的群 G 的阶.

5.67 如果 X 是一个非空集合，定义 $\Omega(X)$ 为 X 上一切正字 ω 的集合；即 $\Omega(X)$ 是由一切满足所有 $e_i=1$ 的 $x_1^{e_1}\cdots x_n^{e_n}$ 组成的 $\mathcal{W}(X)$ 的子集. 定义**自由幺半群**，并证明 $\Omega(X)$ 是以 X 为基的自由幺半群.

5.6 尼尔森-施赖埃尔定理

我们现在要证明关于自由群的最基本的结果之一：自由群的每个子群也是自由的. 这个定理首先于 1921 年由尼尔森 (J. Nielsen) 对有限生成子群进行了证明，1926 年施赖埃尔取消了有限性的假设，所以这个定理现在称为尼尔森-施赖埃尔定理. 尼尔森的方法实际上给出了一个算法，类似于线性代数中的高斯消元法，它用 $\langle A\rangle$ 的基代替自由群 F 的生成集 A[⊖]. 特别地，如果 S 是自由群 F 的有限生成子群，则尼尔森算法把 S 的任一生成集换成 S 的基，由此证明 S 是自由的. 关于这个证明的详情，读者可参考 Lyndon 和 Schupp 的书 4～13 页.

第二种类型的证明于 1933 年由白尔 (R. Baer) 和莱维 (F. Levi) 发现. 该证明运用了拓扑空间 X 的覆盖空间 $\widetilde{X}$ 和它的基本群 $\pi_1(X)$ 的子群之间的一种联系，它类似于伽罗瓦群和中间域之间的对应. 特别地，如果 X 是图 (由边和顶点构成的空间)，则可以证明每个覆盖空间也是图. 由此 $\pi_1(\widetilde{X})$ 同构于 $\pi_1(X)$ 的一个子群. 反之，给定任意一个子群 $S\leqslant\pi_1(X)$，存在 X 的覆盖空间 $\widetilde{X}_S$ 满足 $\pi_1(\widetilde{X}_S)$ 同构于 S. 此外，当 X 是图时，$\pi_1(X)$ 是自由群. 所有这些事实一旦建立后，证明进行如下. 给定自由群 F，存在图 X (一个"圆束") 满足 $F\cong\pi_1(X)$；给定一个子群 $S\leqslant F$，我们知道 $S\cong\pi_1(\widetilde{X}_S)$. 但 $\widetilde{X}_S$ 也是图，从而 $\pi_1(\widetilde{X}_S)$ 且因此 S 是自由的. 有几种避开拓扑的证明，例如在《An Introduction to the Theory of Groups》一书中 377—384 页就展示了一个这种证明. 这一思想的重要变异属于塞尔 (J.-P. Serre)，在他的书《Trees》中用自由群在树 (作为连通图的某种通用覆盖空间产生树) 上的作用刻画了自由群，而 P. J. Higgins 使用了群胚.

我们给出子群定理的 A. J. Weir 的证明 ["The Reidemeister-Schreier and Kuroš Subgroup Theorems", *Mathematika* 3 (1956), 47～55]，因为它比其他证明需要的预备知识少. 该思想来自赖德迈斯特-施赖埃尔 (Reidemeister-Schreier) 定理的证明，这个定理用群 G 的给定的表现给出 G 的子群的表现.

311

定义 设 S 是群 G 的子群，S 在 G 中的一个**陪集代表系** ℓ 是指 G 的这样一个子集，它由每个陪集 Sb 中恰好取出的一个元素 $\ell(Sb)\in Sb$ 组成，且满足 $\ell(S)=1$.

设 F 是以 X 为基的自由群，并设 S 是 F 的子群. 给定 S 在 F 中的一个陪集代表系 ℓ，则对每个 $x\in X$，$\ell(Sb)x$ 和 $\ell(Sbx)$ 都在陪集 Sbx 中，从而

$$t_{Sb,x}=\ell(Sb)x\,\ell(Sbx)^{-1}$$

在 S 中. 我们要证明如果谨慎地选取陪集代表系 ℓ，则不等于 1 的一切 $t_{Sb,x}$ 的集合形成 S 的一组

⊖ 这个理论算法已经发展为 Schreier-Sims 算法，当 S_n 的子群 H 的生成集给出后，它是计算子群 H 的阶的一个有效方法，它也可以判定一个特定的置换是否在 H 中.

基，因此 S 是自由的．

设 ℓ 是自由群 F 的子群 S 的一个陪集代表系，元素 $t_{Sb,x}$ 如上，定义 Y 为符号 $y_{Sb,x}$ 上的自由群，从而 $y_{Sb,x}\mapsto t_{Sb,x}$ 是双射．定义 $\varphi: Y\to S$ 为

$$\varphi: y_{Sb,x}\mapsto t_{Sb,x} = \ell(Sb)x\,\ell(Sbx)^{-1}$$

的同态．我们先定义**陪集函数** $F\to Y$，对每个陪集 Sb 定义一个，记为 $u\mapsto u^{Sb}$．这些函数不是同态，我们对 $|u|\geqslant 0$ 用归纳法同时定义它们，其中 u 是 X 上的约化字．对一切 $x\in X$ 和一切陪集 Sb，定义

$$1^{Sb} = 1, x^{Sb} = y_{Sb,x} \text{ 和 } (x^{-1})^{Sb} = (x^{Sbx^{-1}})^{-1}.$$

如果 $u=x^{\epsilon}v$ 是长度为 $n+1$ 的约化字，其中 $\epsilon=\pm 1$ 和 $|v|=n$，定义

$$u^{Sb} = (x^{\epsilon})^{Sb}v^{Sbx^{\epsilon}}.$$

引理 5.84　（i）对一切 $u,v\in F$，陪集函数满足 $(uv)^{Sb} = u^{Sb}v^{Sbu}$．

（ii）对一切 $u\in F$，$(u^{-1})^{Sb} = (u^{Sbu^{-1}})^{-1}$.

（iii）如果 $\varphi: Y\to S$ 是同态 $\varphi: y_{Sb,x}\mapsto t_{Sb,x} = \ell(Sb)x\,\ell(Sbx)^{-1}$，则对一切 $u\in F$，$\varphi(u^{Sb}) = \ell(Sb)u\,\ell(Sbu)^{-1}$.

（iv）由 $\theta: u\mapsto u^{S}$ 给出的函数 $\theta: S\to Y$ 是同态，且 $\varphi\theta=1_S$.

证明　（i）对 $|u|$ 用归纳法证明，其中 u 是约化字．如果 $|u|=0$，则 $u=1$ 和 $(uv)^{Sb} = v^{Sb}$；另一方面，$1^{Sb}v^{Sb1} = v^{Sb}$.

关于归纳步，记 $u = x^{\epsilon}w$，则

$$\begin{aligned}(uv)^{Sb} &= (x^{\epsilon})^{Sb}(wv)^{Sbx^{\epsilon}} && \text{（陪集函数的定义）}\\ &= (x^{\epsilon})^{Sb}w^{Sbx^{\epsilon}}v^{Sbx^{\epsilon}w} && \text{（归纳假设）}\\ &= (x^{\epsilon})^{Sb}w^{Sbx^{\epsilon}}v^{Sbu}\\ &= (x^{\epsilon}w)^{Sb}v^{Sbu}\\ &= u^{Sb}v^{Sbu}.\end{aligned}$$

312

（ii）结论由

$$1 = 1^{Sb} = (u^{-1}u)^{Sb} = (u^{-1})^{Sb}u^{Sbu^{-1}}$$

得到．

（iii）注意到 Y 是以一切 $y_{Sb,x}$ 为基的自由群，从而 φ 定义了一个同态．也对 $|u|\geqslant 0$ 用归纳法证明．首先 $\varphi(1^{Sb}) = \varphi(1) = 1$，而 $\ell(S)1\,\ell(S1)^{-1} = 1$.

关于归纳步，记 $u = x^{\epsilon}v$，其中 u 是约化字．则

$$\begin{aligned}\varphi(u^{Sb}) = \varphi(((x^{\epsilon}v)^{Sb}) &= \varphi((x^{\epsilon})^{Sb}v^{Sbx^{\epsilon}})\\ &= \varphi((x^{\epsilon})^{Sb})\varphi(v^{Sbx^{\epsilon}})\\ &= \varphi((x^{\epsilon})^{Sb})\,\ell(Sbx^{\epsilon})v\,\ell(Sbx^{\epsilon}v)^{-1},\end{aligned}$$

其中最后一个等式来自归纳假设．现在关于 ϵ 的符号有两种情形．如果 $\epsilon=+1$，则

$$\begin{aligned}\varphi(u^{Sb}) &= \ell(Sb)x\,\ell(Sbx)^{-1}\,\ell(Sbx)v\,\ell(Sbxv)^{-1}\\ &= \ell(Sb)xv\,\ell(Sbxv)^{-1}\\ &= \ell(Sb)u\,\ell(Sbu)^{-1}.\end{aligned}$$

如果 $\epsilon=-1$，则

$$\begin{aligned}\varphi(u^{Sb}) &= \varphi((y_{Sbx^{-1},x})^{-1})\ \ell(Sbx^{-1})v\ell(Sbx^{-1}v)^{-1} \\ &= (\ \ell(Sbx^{-1})x\ell(Sbx^{-1}x)^{-1})^{-1}\ \ell(Sbx^{-1})v\ell(Sbx^{-1}v)^{-1} \\ &= \ell(Sb)x^{-1}\ \ell(Sbx^{-1})^{-1}\ \ell(Sbx^{-1})v\ell(Sbx^{-1}v)^{-1} \\ &= \ell(Sb)x^{-1}v\ell(Sbx^{-1}v)^{-1} \\ &= \ell(Sb)u\ell(Sbu)^{-1}.\end{aligned}$$

（ⅳ）对 $u\in S$，定义 $\theta: S\to Y$ 为

$$\theta: u\mapsto u^S$$

（当然，θ 是 $b=1$ 时陪集函数 $u\mapsto u^{Sb}$ 对 S 的限制）．现在，如果 $u,v\in S$,则当 $u\in S$时，因为 $Su=S$，从而

$$\theta(uv) = (uv)^S = u^S v^{Su} = u^S v^S = \theta(u)\theta(v),$$

所以 θ 是同态．此外，如果 $u\in S$，则（ⅲ）给出

313

$$\varphi\theta(u) = \varphi(u^S) = \ell(S1)u\ell(S1u)^{-1} = u. \qquad ■$$

系 5.85 如果 S 是自由群 F 的子群，并且 ℓ 是 S 在 F 中的陪集代表系，则不等于1的一切 $t_{Sb,x}$ 的集合生成 S.

证明 因复合 $\varphi\theta=1_S$，所以函数 $\varphi: Y\to S$ 是满射,因此 Y 的生成元 $y_{Sb,x}$ 的象 $t_{Sb,x}$ 生成 $\mathrm{im}\varphi=S$. 当然，可以删去生成集中出现的1. ■

下一引理证明 S 有表现

$$S=(y_{Sb,x},\text{一切 } x\in X,\text{一切陪集 } Sb\mid \ell(Sb)^S,\text{一切陪集 } Sb).$$

引理 5.86 如果 ℓ 是 S 在 F 中的陪集代表系，则 $\ker\varphi$ 是由一切 $\ell(Sb)^S$ 生成的 Y 的正规子群.

证明 设 N 由一切 $\ell(Sb)^S$ 生成的 Y 的正规子群，并设 $K=\ker\varphi$. 根据引理 5.84(ⅳ)，$\theta: S\to Y$ 是同态且满足 $\varphi\theta=1_S$（其中 $\varphi: y_{Sb,x}\mapsto t_{Sb,x}$ 和 $\theta: u\mapsto u^S$）. 根据习题5.72(ⅱ)，K 是由 $\{y^{-1}\rho(y): y\in Y\}$ 生成的 Y 的正规子群，其中 $\rho=\theta\varphi$. 根据引理5.84(ⅰ)，

$$\begin{aligned}y_{Sb,x}^{-1}\rho(y_{Sb,x}) &= y_{Sb,x}^{-1}(\ \ell(Sb)x\ \ell(Sbx)^{-1})^S \\ &= y_{Sb,x}^{-1}\ \ell(Sb)^S x^{Sb}(\ \ell(Sbx)^{-1})^{Sbx} \\ &= (y_{Sb,x}^{-1}\ \ell(Sb)^S y_{Sb,x})(\ \ell(Sbx)^{-1})^{Sbx},\end{aligned}$$

其中 $x^{Sb}=y_{Sb,x}$是陪集函数 $u\to u^{Sb}$ 定义中的一个等式．由于引理5.84(ⅱ)给出 $(\ \ell(Sbx)^{-1})^{Sbx}=(\ \ell(Sbx)^S)^{-1}$，所以

$$y_{Sb,x}^{-1}\rho(y_{Sb,x}) = (y_{Sb,x}^{-1}\ \ell(Sb)^S y_{Sb,x})(\ \ell(Sbx)^S)^{-1}. \tag{1}$$

由等式 (1)，$y_{Sb,x}^{-1}\rho(y_{Sb,x})\in N$, 从而 $K\leqslant N$. 关于反包含，等式 (1) 说明 $\ell(Sb)^S\in K$ 当且仅当 $\ell(Sbx)^S\in K$. 因此所要的包含关系可以对 $|\ell(Sb)|$ 用归纳法证明，从而 $K=N$. ■

我们现在选择一个特定的陪集代表系．

定义 设 F 是以 X 为基的自由群，并设 S 是 F 的子群．一个**施赖埃尔陪集代表系**是指满足下列性质的陪集代表系 ℓ：如果 $\ell(Sb)=x_1^{e_1}x_2^{e_2}\cdots x_n^{e_n}$ 是约化字，则每个初始段 $x_1^{e_1}x_2^{e_2}\cdots x_k^{e_k}$ 也在陪集代表系中，其中 $1\leqslant k\leqslant n$.

引理 5.87 对 F 的每个子群 S 都存在施赖埃尔陪集代表系．

314

证明 定义陪集 Sb 的**长度**为元素 $sb\in Sb$ 的最小长度，记为 $|Sb|$．我们对 $|Sb|$ 用归纳法证明

存在代表元$\ell(Sb)\in Sb$使得它的一切初始段都是长度较短的陪集的代表元．一开始定义$\ell(S)=1$. 关于归纳步，设$|Sz|=n+1$和$ux^{\epsilon}\in Sz$,其中$\epsilon=\pm1$和$|ux^{\epsilon}|=n+1$. 现在如果$|Su|=m<n$，就会有一个长度为m的代表元v，且vx^{ϵ}将是Sz的代表元，但vx^{ϵ}的长度$<n+1$，所以必有$|Su|=n$. 由归纳假设，存在$b=\ell(Su)$使得它的每个初始段也是代表元．定义$\ell(Sz)=bx^{\epsilon}$. ■

下面是我们一直所寻求的结果．

定理 5.88（尼尔森-施赖埃尔） 自由群F的每个子群S都是自由的．事实上，如果X是F的基，ℓ是S在F中的施赖埃尔陪集代表系，则S的一个基由一切不等于1的$t_{Sb,x}=\ell(Sb)x\,\ell(Sbx)^{-1}$组成．

证明 回忆$S\cong Y/K$，其中Y是以一切符号$y_{Sb,x}$为基的自由群，且$K=\ker\varphi$；根据引理5.86，K等于由一切$\ell(Sb)^S$生成的正规子群．根据习题5.58，只需证明K等于由一切**特定的**$y_{Sb,x}$生成的Y的正规子群T；即满足$\varphi(y_{Sb,x})=t_{Sb,x}=1$的那些$y_{Sb,x}$. 显然，$T\leqslant K=\ker\varphi$，因此只需证明反包含．我们对$|\ell(Sv)|$用归纳法证明$\ell(Sv)^S$是特定的$y_{Sb,x}$上的字．如果$|\ell(Sv)|=0$，则$\ell(Sv)=\ell(S)=1$，它是特定的$y_{Sb,x}$上的字．如果$|\ell(Sv)|>0$，则$\ell(Sv)=ux^{\epsilon}$，其中$\epsilon=\pm1$和$|u|<|\ell(Sv)|$．因$\ell$是施赖埃尔陪集代表系，所以$u$也是一个代表元：$u=\ell(Su)$. 根据引理5.84（ⅰ），

$$\ell(Sv)^S=u^S(x^{\epsilon})^{Su}.$$

由归纳假设，u^S是特定$y_{Sb,x}$上的字，因此$u^S\in T$.

剩下的是证明$(x^{\epsilon})^{Su}$是特定$y_{Sb,x}$上的字．如果$\epsilon=\pm1$，则$(x^{\epsilon})^{Su}=x^{Su}=y_{Su,x}$. 但因为$v=ux$且$\ell$是施赖埃尔陪集代表系，所以有$\ell(Sux)=ux$，从而

$$\varphi(y_{Su,x})=t_{Su,x}=\ell(Su)x\,\ell(Sux)^{-1}=ux(ux)^{-1}=1.$$

所以$y_{Su,x}$是特定$y_{Sb,x}$中的一个且x^{Su}在T中．如果$\epsilon=-1$，则陪集函数的定义给出

$$(x^{-1})^{Su}=(x^{Sux^{-1}})^{-1}=(y_{Sux^{-1},x})^{-1}.$$

因此，

$$\varphi((x^{-1})^{Su})=(t_{Sux^{-1},x})^{-1}=[\ell(Sux^{-1})x\ell(Sux^{-1}x)]^{-1}=[\ell(Sux^{-1})x\,\ell(Su)]^{-1}.$$

因ℓ是施赖埃尔陪集代表系，所以有$\ell(Su)=u$和$\ell(Sux^{-1})=\ell(Sv)=v=ux^{-1}$. 由此，

$$\varphi((x^{-1})^{Su})=[(ux^{-1})xu^{-1}]^{-1}=1.$$

所以$y_{Sux^{-1},x}$是特定的$y_{Sb,x}$中的一个，从而$(x^{-1})^{Su}\in T$，证明完成． ■

下面是尼尔森-施赖埃尔定理的一个很好的应用．

315

系 5.89 设F是自由群，$u,v\in F$,则u,v可交换当且仅当存在$z\in F$使得$u,v\in\langle z\rangle$.

证明 充分性显然成立，如果$u,v\in\langle z\rangle$，则它们都在一个阿贝尔群中，因此它们可交换．

反之，尼尔森-施赖埃尔定理说子群$\langle u,v\rangle$是自由的．另一方面，u,v可交换的条件说$\langle u,v\rangle$是阿贝尔群，但根据习题5.59（ⅱ），一个阿贝尔自由群必是循环群，所以正如要证的，$\langle u,v\rangle\cong\mathbb{Z}$. ■

下一结果表明，和阿贝尔群相反，有限生成群的子群未必是有限生成的．

系 5.90 如果F是秩为2的自由群，则它的换位子群F'是秩为无限的自由群．

证明 设$\{x,y\}$是F的基．根据引理5.74，F/F'是以$\{xF',yF'\}$为基的自由阿贝尔群，因此每个陪集$F'b$有唯一的形如x^my^n的代表元，其中$m,n\in\mathbb{Z}$. 因为x^my^n的每个子字是有同样形式的字，所以选取$\ell(F'b)=x^my^n$的陪集代表系是施赖埃尔陪集代表系．如果$n>0$，则$\ell(F'y^n)=y^n$，而

$\ell(F'y^n x) = xy^n \neq y^n x$. 所以有无限个元素 $t_{Sy^n,x} = \ell(F'y^n)x\,\ell(F'y^n x)^{-1} \neq 1$，于是从尼尔森-施赖埃尔定理可得结论． ■

即使有限生成自由群的任一子群未必是有限生成的，但指数有限的子群必是有限生成的．

系 5.91 *如果 F 是有有限秩 n 的自由群，则 F 的每个具有有限指数 j 的子群 S 也是有限生成的．事实上，$\text{rank}(S) = jn - j + 1$.*

证明 设 $X = \{x_1, \cdots, x_n\}$ 是 F 的基，并设 $\ell = \{\ell(Sb)\}$ 是施赖埃尔陪集代表系．根据定理 5.88，S 的一组基由不等于 1 的那些元素 $t_{Sb,x}$ 组成，其中 $x \in X$. Sb 有 j 种取法，x 有 n 种取法，所以 S 的基中最多有 jn 个元素，因此 $\text{rank}(S) \leqslant jn$，从而 S 是有限生成的．

有序对 (Sb, x) 称为**平凡的**，如果 $t_{Sb,x} = 1$，即 $\ell(Sb)x = \ell(Sbx)$. 我们要证明在陪集族 $\{Sb \neq S\}$ 和平凡有序对之间存在双射ψ，从而有 $j-1$ 个平凡有序对．由此可知

$$\text{rank}(S) = jn - (j-1) = jn - j + 1.$$

因 $Sb \neq S$，有$\ell(Sb) = b = ux^{\epsilon}$. 因$\ell$是施赖埃尔陪集代表系，有 $u \in \ell$. 定义 $\psi(Sb)$ 如下：

$$\psi(Sux^{\epsilon}) = \begin{cases} (Su, x) & \text{如果 } \epsilon = +1; \\ (Sux^{-1}, x) & \text{如果 } \epsilon = -1. \end{cases}$$

注意 $\psi(Sux^{\epsilon})$ 是平凡有序对．如果 $\epsilon = +1$，则 $\ell(Sux) = \ell(Sb) = b = ux$，从而 $\ell(Su)x = ux$ 和 $t_{Su,x} = 1$. 如果 $\epsilon = -1$，则 $\ell(Sbx) = \ell(Sux^{-1}, x) = \ell(Su) = u$，从而 $\ell(Sb)x = bx = ux^{-1}x = u$ 和 $t_{Sb,x} = 1$.

316

为证明ψ是单射，假设 $\psi(Sb) = \psi(Sc)$，其中 $b = ux^{\epsilon}$ 和 $c = vy^{\eta}$，我们假定 x, y 在 F 的给定基中且 $\epsilon = \pm 1$，$h = \pm 1$. 根据 ϵ 和η的符号有四种可能性．

$$(Su, x) = (Sv, y);\ (Su, x) = (Svy^{-1}, y);\ (Sux^{-1}, x) = (Sv, y);\ (Su, x) = (Svy^{-1}, y).$$

在每种情形中，有序对的相等给出 $x = y$. 如果 $(Su, x) = (Sv, x)$，则 $Su = Sv$，因此正如所要的 $Sb = Sux = Svx = Sc$. 如果 $(Su, x) = (Svx^{-1}, x)$，则 $Su = Svx^{-1} = Sc$，从而 $\ell(Su) = \ell(Sc) = c$. 但因 (Su, x) 是平凡有序对，所以有 $\ell(Su)x = \ell(Sux) = b$. 因此 $b = \ell(Su)x = cx = vx^{-1}x$，与 b 是约化字（和施赖埃尔陪集代表系中的任一元素一样）矛盾．同样的矛盾表明不可能有 $(Sux^{-1}, x) = (Sv, x)$. 最后，如果 $(Sux^{-1}, x) = (Svx^{-1}, x)$，则 $Sb = Sux^{-1} = Svx^{-1} = Sc$.

为证明ψ是满射，取一个平凡有序对 (Sw, x)，即 $\ell(Sw)x = wx = \ell(Swx)$. 现在 $w = ux^{\epsilon}$，其中 $u \in \ell$，$\epsilon = \pm 1$. 如果 $\epsilon = +1$，则 w 不以 x^{-1}结尾，从而 $\psi(Swx) = (Sw, x)$. 如果 $\epsilon = -1$，则 w 以 x^{-1}结尾，从而 $\psi(Su) = (Sux^{-1}, x) = (Sw, x)$. ■

系 5.92 *存在不同构的有限生成群 G 和 H，它们的每一个同构于另一个的子群．*

证明 如果 G 是秩为 2 的自由群，H 是秩为 3 的自由群，则 $G \ncong H$. 显然 G 与 H 的一个子群同构．另一方面，换位子群 G'是秩无限的自由群，从而 G'包含秩为 3 的自由子群，因此 G 也包含秩为 3 的自由子群，即 H 与 G 的子群同构． ■

我们处在一个叫做**组合群论**的内容丰富的主题的起始点上，它研究对于给定的群表现能说出多少关于这个群的事情．最值得注意的结果之一是字问题的不可解性．如果群 G 有表现 $G = (X \mid R)$，它存在判定 X 上的任意字 w 是否等于 G 中幺元元素的算法（如果 X 和 R 都是有限的，可以证明这个性质不依赖于表现的选取），则称群 G 有**可解的字问题**．20 世纪 50 年代末，诺维科夫 (P. S. Novikov) 和布恩（W. W. Boone）独立地证明了存在没有可解字问题的有限表现群 G（见罗特曼所著的《An Introduction to the Theory of Groups》第 12 章）．其他问题牵涉到寻找已知群的表

现，如同我们对 $\mathbf{Q}_n$ 和 D_{2n} 所做的那样；这些问题的一本极好的参考书是 Coxeter-Moser 所著的《Generators and Relations for Discrete Groups》．另一个问题是由表现定义的一个群是有限的还是无限的．例如，**伯恩赛德问题**问具有有限指数 m 的有限生成群是否必定有限，所谓一个群有指数 m 是指对一切 $x \in G$ 有 $x^m=1$ [伯恩赛德已经证明：如果这样的群 G 对某个 n 是 $\mathrm{GL}(n,X)$ 的子群，则 G 有限]．然而一般的回答是否定的；这样的群可以是无限的．对大奇数 m，首先由诺维科夫和 S. I. Adyan 在一篇长而复杂的论文中予以证明．运用涉及范坎彭图的几何技巧（关于这个课题的一个导引可见 Lyndon-Schupp 所著的《Combinatorial Group Theory》），A. Yu. Ol'shanskii给出一个简短得多的证明．最后伊万诺夫（S. V. Ivanov）通过证明当 m 是大偶数时，表现群可以是无限的完成了这个问题的解．另一个几何技巧涉及有限生成群 G 的**凯莱图**，这是一个依赖于给定的有限生成集的图；可以证明 G 是自由的当且仅当它有作为树的凯莱图（见塞尔所著的《Trees》）．最后，表现和算法之间的相互关系具有理论和应用两方面的意义．希格曼（G. Higman）的一个定理（见 Rotman 所著的《An Introduction to the Theory of Groups》第 12 章）称一个有限生成群 G 可以作为一个有限表现群 H 的子群嵌入（即 H 具有有限个生成元和有限个关系的表现）当且仅当 G 是*递归表现*的：G 有这样的表现，它的关系可以由一个算法给出．在应用方面，解决群论问题的许多有效算法已经实现，见 Sims 所著的《Computation with Finitely Presented Groups》．第一个算法是**陪集计数**（见 Lyndon-Schupp 所著的《Combinatorial Group Theory》163～167 页），它计算了当 $|G|$ 有限时，由表现定义的群 G 的阶（不幸的是，可能没有算法可以预先判定 G 是否有限）．

317

习题

5.68 设 G 是有限生成群，且设 $H \leqslant G$ 有有限指数．证明 H 是有限生成的．

5.69 证明：如果 F 是有有限秩 $n \geqslant 2$ 的自由群，则它的换位子群 F' 是有无限秩的自由群．

5.70 设 G 是非循环群的有限群．如果 $G \cong F/S$，其中 F 是秩有限的自由群，证明 $\mathrm{rank}(S) > \mathrm{rank}(F)$.

5.71 (i) 证明：如果 G 是由两个 2 阶元素 a 和 b 生成的有限群，则对某个 $n \geqslant 2$ 有 $G \cong D_{2n}$.

(ii) 设 $G = \langle A,B \rangle \leqslant \mathrm{GL}(2,\mathbb{Q})$，其中

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{和 } B = \begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}.$$

证明 $A^2 = I = B^2$，但 AB 的阶无限．（模群给出群的另一个例子，其中两个有限阶元素之积的阶无限．）这个群 G 通常记为 D_∞，叫做**无限二面体群**．

5.72 设 Y 和 S 是群，并设 $\varphi: Y \to S$ 和 $\theta: S \to Y$ 是同态满足 $\varphi\theta = 1_S$.

(i) 如果 $\rho: Y \to Y$ 定义为 $\rho = \theta\varphi$，证明 $\rho\rho = \rho$ 以及对每个 $a \in \mathrm{im}\theta, \rho(a) = a$.（同态 ρ 叫做**收缩**．）

(ii) 如果 K 是 Y 的正规子群，它由一切 $y^{-1}\rho(y)$ 生成，其中 $y \in Y$，证明 $K = \ker\varphi$.

提示：注意，因为 θ 是单射，所以 $\ker\varphi = \ker\rho$. 对一切 $y \in Y$ 用等式 $y = \rho(y)(\rho(y)^{-1})y$.

318

第6章 交换环 Ⅱ

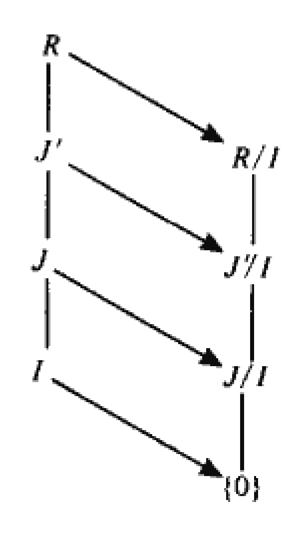
本章我们主要的兴趣是研究多元多项式．照例，在涉及多项式环之前，先考虑更一般的设置（在这里就是交换环）比较简单．交换环中理想的本性十分重要：例如我们已经看到在 PID 中存在 gcd，而且它们是线性组合，但在其他环中未必享有这些性质．三个特殊类型的理想——素理想、极大理想和有限生成理想——是最重要的．称一个交换环为*诺特环*，如果每个理想都是有限生成的，希尔伯特基定理证明 $k[x_1,\cdots,x_n]$ 是诺特环，其中 k 是域．其次，我们收集了佐恩引理（在附录中讨论）的几种重要应用，例如极大理想的存在性（这是科恩（I. S. Cohen）的一个定理，该定理说一个交换环是诺特环当且仅当每个素理想是有限生成的），域的代数闭包的存在性和唯一性，超越基的存在性（以及吕罗特定理）和极大可分扩张的存在性．其后，介绍一种几何观点，其中理想对应于某种叫做*簇*的仿射子集，这一讨论牵涉零点定理和准素分解．最后，在末尾一节介绍格罗布纳基的概念，它把带余除法从 $k[x]$ 扩张到 $k[x_1,\cdots,x_n]$，并由此产生一个实用算法，它可以解决许多能翻译成多元多项式语言的问题．

6.1 素理想和极大理想

我们已经呈示的数论的大量内容牵涉到整除性：给定两个整数 a 和 b，什么时候 $a\mid b$，即什么时候 a 是 b 的因数？这个问题可以转化为有关主理想的问题，因为 $a\mid b$ 当且仅当 $(b)\subseteq(a)$．我们现在引入理想的两个特别重要的类型：*素理想*（它与欧几里得引理相关）和*极大理想*．

319

我们先从类似于群的对应定理即定理 2.76 的一个定理开始．



命题 6.1（环的对应定理） *如果 I 是交换环 R 的一个真理想，则在包含 I 的一切中间理想 J（即 $I\subseteq J\subseteq R$）的集合到 R/I 中的一切理想的集合之间，存在保持包含关系的双射 φ，该双射由*

$$\varphi: J\mapsto \pi(J)=J/I=\{a+I: a\in J\}$$

给出，其中 $\pi: R\to R/I$ 是自然映射．

证明 如果忘记它的乘法，交换环 R 只是一个加法阿贝尔群，而它的理想 I 是一个（正规）子群．现在运用群的对应定理，即定理 2.76，可以给出一个保持包含关系的双射

$$\Phi:\{R\text{ 包含 }I\text{ 的一切子群}\}\to\{R/I\text{ 的一切子群}\},$$

其中 $\Phi(J)=\pi(J)=J/I$．

如果 J 是理想，则 $\Phi(J)$ 也是理想，这是因为如果 $r\in R$ 和 $a\in J$，则 $ra\in J$，从而

$$(r+I)(a+I)=ra+I\in J/I.$$

令 φ 是 Φ 在中间理想的集合上的限制，因为 Φ 是双射，所以 φ 是单射．为证明 φ 是满射，设 J^* 是 R/I 中的理想．现在 $\pi^{-1}(J^*)$ 是 R 中的中间理想[它包含 $I=\pi^{-1}(\{0\})$]，根据命题 1.50(ⅱ)，$\varphi(\pi^{-1}(J^*))=\pi(\pi^{-1}(J^*))=J^*$． ■

实际应用中，把商环 R/I 中的每个理想说成有 J/I 的形式，其中 J 是满足 $I\subseteq J\subseteq R$ 的某个唯

一确定的理想，就是默默地调用了对应定理．

例 6.2 设 $I=(m)$ 是$\mathbb{Z}$中的非零理想．如果 J 是$\mathbb{Z}$中包含 I 的一个理想，则有某个 $a\in\mathbb{Z}$ 使得 $J=(a)$，这是因为$\mathbb{Z}$是一个 PID，且 $(m)\subseteq(a)$ 当且仅当 $a\mid m$．因为 $J/I=([a])$，其中 a 是 m 的某个因数，对应定理现在表明环$\mathbb{I}_m$ 中的每个理想都形如 $([a])$． ■ [320]

定义 *交换环 R 中的理想 I 称为*素理想，*如果它是真理想，即 $I\neq R$，且 $ab\in I$ 蕴涵 $a\in I$ 或 $b\in I$.*

例 6.3 （ⅰ）回忆非零交换环 R 是整环当且仅当在 R 中 $ab=0$ 蕴涵 $a=0$ 或 $b=0$. 于是，R 中的理想 $(0)=\{0\}$ 是素理想当且仅当 R 是整环．

（ⅱ）我们断言$\mathbb{Z}$中的素理想正好就是理想 (p)，其中 $p=0$ 或 p 是素数．因 m 和 $-m$ 生成同一主理想，我们可以只关注非负生成元．如果 $p=0$，则因为$\mathbb{Z}$是整环，由（ⅰ）可得结果．如果 $p>0$，我们先证明 (p) 是真理想．否则，$1\in(p)$，于是有整数 a 使得 $ap=1$，这是一个矛盾．其次，如果 $ab\in(p)$，则 $p\mid ab$. 根据欧几里得引理，$p\mid a$ 或 $p\mid b$，即 $a\in(p)$ 或 $b\in(p)$．所以 (p) 是素理想．

反之，如果 $m>1$ 不是素数，则它有因数分解 $m=ab$，其中 $0<a<m$ 和 $0<b<m$，于是 a 和 b 都不是 m 的倍数，从而都不在 (m) 中．但 $ab=m\in(m)$，所以 (m) 不是素理想． ■

命题 6.4 *交换环 R 的理想 I 是素理想当且仅当 R/I 是整环．*

证明 设 I 是素理想．因 I 是真理想，所以有 $1\notin I$，从而在 R/I 中，$1+I\neq 0+I$．如果 $0=(a+I)(b+I)=ab+I$，则 $ab\in I$．因 I 是素理想，所以 $a\in I$ 或 $b\in I$，即 $a+I=0$ 或 $b+I=0$．因此 R/I 是整环．逆命题容易证明． ■

例6.3(ⅱ)中对素数的刻画可以扩展到系数在某个域中的多项式．

命题 6.5 *如果 k 是域，则一个非零多项式 $p(x)\in k[x]$ 是不可约的当且仅当 $(p(x))$ 是素理想．*

证明 假设 $p(x)$ 是不可约的．首先，(p) 是真理想，否则 $k[x]=(p)$，因此 $1\in(p)$，从而存在多项式 $f(x)$ 使得 $1=p(x)f(x)$．但 $p(x)$ 的次数至少是 1，而

$$0=\deg(1)=\deg(pf)=\deg(p)+\deg(f)\geqslant\deg(p)\geqslant 1.$$

这个矛盾表明 (p) 是真理想．其次，如果 $ab\in(p)$，则 $p\mid ab$，因此 $k[x]$ 中的欧几里得引理给出 $p\mid a$ 或 $p\mid b$．于是 $a\in(p)$ 或 $b\in(p)$，由此，(p) 是素理想．

反之，如果 $(p(x))$ 是素理想，则 $fg\in(p)$ 蕴涵 $f\in(p)$ 或 $g\in(p)$，即 $p\mid f$ 或 $p\mid g$．所以欧几里得引理对 p 成立，习题 3.31 证明 p 是不可约的． ■ [321]

如果 I 是交换环 R 中的理想，而且 I 还是 R 的真理想，我们记为 $I\subsetneq R$. 更一般地，如果 I 和 J 都是理想，我们用 $I\subsetneq J$ 表示 $I\subseteq J$ 且 $I\neq J$.

下面是理想的第二个重要类型．

定义 *交换环 R 中的理想 I 称为*极大理想，*如果它是真理想且不存在理想 J 满足 $I\subsetneq J\subsetneq R$.*

由此，如果 I 是交换环 R 中的极大理想，且 J 是真理想满足 $I\subseteq J$，则 $I=J$. 每个交换环 R 都包含极大理想吗？这个问题的（正面）答案牵涉佐恩引理，我们将在 6.4 节中讨论．

例 6.6 交换环 R 中的理想 $\{0\}$ 是极大理想当且仅当 R 是域．例3.51(ⅱ)证明 R 中的每个非零理想 I 等于 R 本身当且仅当 R 中的每个非零元素都是单位，即 $\{0\}$ 是极大理想当且仅当 R 是域． ■

命题 6.7 *非零交换环 R 中的真理想 I 是极大理想当且仅当 R/I 是域．*

证明 环的对应定理表明 I 是极大理想当且仅当 R/I 没有除 $\{0\}$ 和 R/I 自身外的其他理想．例 6.6 证明这个性质成立当且仅当 R/I 是域．（注意，因在域中 $1\neq0$，I 必是真理想．） ■

系 6.8 *交换环 R 中的每个极大理想 I 都是素理想．*

证明 如果 I 是极大理想，则 R/I 是域．因每个域都是整环，所以 R/I 是整环，因此 I 是素理想． ■

多项式环 $k[x_1,\cdots,x_n]$ 中的素理想可能十分复杂，但当 k 是一个代数闭域时，定理 6.102 表明每个极大理想都形如 $(x_1-a_1,\cdots,x_n-a_n)$，其中 $(a_1,\cdots,a_n)$ 是 k^n 中的某个点，即当 k 是代数闭域时，k^n 和 $k[x_1,\cdots,x_n]$ 中一切极大理想的集合之间存在双射．

例 6.9 系 6.8 的逆命题不成立．例如考虑$\mathbb{Z}[x]$中的主理想 (x)．根据习题 3.83，有

$$\mathbb{Z}[x]/(x)\cong\mathbb{Z};$$

因$\mathbb{Z}$是整环，所以 (x) 是素理想．因$\mathbb{Z}$不是域，所以 (x) 不是极大理想．不难举出一个真理想 J 严格包含 (x)．令

$$J=\{f(x)\in\mathbb{Z}[x]:f(x)\text{ 的常数项为偶数}\}.$$

322 因$\mathbb{Z}[x]/J\cong\mathbb{F}_2$是域，从而 J 是包含 (x) 的极大理想． ■

例 6.10 设 k 是域，并设 $a=(a_1,\cdots,a_n)\in k^n$. 定义**赋值映射**

$$e_a:k[x_1,\cdots,x_n]\to k$$

为

$$e_a:f(x_1,\cdots,x_n)\mapsto f(a)=f(a_1,\cdots,a_n).$$

在例3.46(ⅳ)中我们已经看到 e_a 是满射环同态，从而 $\ker e_a$ 是极大理想．现在$(x_1-a_1,\cdots,x_n-a_n)\subseteq\ker e_a$. 然而在习题6.6(ⅰ)中我们看到$(x_1-a_1,\cdots,x_n-a_n)$是极大理想，因此，它必等于 $\ker e_a$. ■

当 R 是 PID 时，系 6.8 的逆命题成立．

定理 6.11 *如果 R 是主理想整环，则每个非零素理想 I 都是极大理想．*

证明 假定有一个真理想 J 满足 $I\subseteq J$. 因 R 是 PID，有某个 a，$b\in R$ 使得 $I=(a)$ 和 $J=(b)$．现在 $a\in J$ 蕴涵有某个 $r\in R$ 使得 $a=rb$，从而 $rb\in I$. 但 I 是素理想，因此 $r\in I$ 或 $b\in I$. 如果 $r\in I$，则有某个 $s\in R$ 使得 $r=sa$，从而 $a=rb=sab$. 因 R 是整环，所以 $1=sb$，并且习题 3.18 给出 $J=(b)=R$，与 J 是真理想的假设矛盾．如果 $b\in I$，则 $J\subseteq I$，从而 $J=I$. 所以 I 是极大理想． ■

我们现在给出命题 3.116 的第二个证明．

系 6.12 *如果 k 是域且 $p(x)\in k[x]$ 是不可约多项式，则商环 $k[x]/(p(x))$ 是域．*

证明 因 $p(x)$ 是不可约的，所以主理想 $I=(p(x))$ 是非零素理想．因 $k[x]$ 是 PID，因此 I 是极大理想，所以 $k[x]/I$ 是域． ■

下面是应用素理想的几种方式．

命题 6.13 *设 P 是交换环 R 中的素理想．如果 I 和 J 都是理想满足 $IJ\subseteq P$，则 $I\subseteq P$ 或 $J\subseteq P$.*

证明 假设相反，$I\nsubseteq P$ 且 $J\nsubseteq P$，由此存在 $a\in I$ 和 $b\in J$ 满足 a，$b\notin P$，而 $ab\in IJ\subseteq P$，与 P 是素理想矛盾． ■

下一结果取自卡普兰斯基（Kaplansky）所著的《Commutative Rings》．

命题 6.14 *设 B 是交换环 R 的一个在加法和乘法下封闭的子集．*

（ⅰ）设 $J_1,\cdots,J_n$ 是 R 中的理想，其中至少有 $n-2$ 个是素理想．如果 $B\subseteq J_1\cup\cdots\cup J_n$，则 B 323 *包含在某个 J_i 中．*

（ⅱ）设 I 是 R 中的理想满足 $I\subsetneq B$. 如果存在素理想 $P_1,\cdots,P_n$ 使得 $B-I\subseteq P_1\cup\cdots\cup P_n$（其中 $B-I$ 是 I 在 B 中的集合论意义下的补集），则有某个 i 使得 $B\subseteq P_i$.

证明 （i）对 $n\geqslant 2$ 用归纳法证明．关于基础步 $n=2$，理想 J_1 和 J_2 两者都不必是素的．如果 $B\nsubseteq J_2$，则存在 $b_1\in B$ 使得 $b_1\notin J_2$．因 $B\subseteq J_1\cup J_2$，必有 $b_1\in J_1$．同样，如果 $B\nsubseteq J_1$，则存在 $b_2\in B$ 使得 $b_2\notin J_1$ 和 $b_2\in J_2$．然而，如果 $y=b_1+b_2$，则 $y\notin J_1$，否则，$b_2=y-b_1\in J_1$（因为 y 和 b_1 都在 J_1 中），这就产生矛盾．同样，$y\notin J_2$，与 $B\subseteq J_1\cup J_2$ 矛盾．

关于归纳步，假定 $B\subseteq J_1\cup\cdots\cup J_{n+1}$，其中至少有 $n-1=(n+1)-2$ 个 J_i 是素理想．令

$$D_i = J_1 \cup \cdots \cup \hat{J}_i \cup \cdots \cup J_{n+1}.$$

因 D_i 是 n 个理想的并，其中至少有 $(n-1)-1=n-2$ 个是素理想，归纳假设允许我们假定对一切 i，$B\nsubseteq D_i$．因此对一切 i，存在 $b_i\in B$ 而 $b_i\notin D_i$．因 $B\subseteq D_i\cup J_i$，必有 $b_i\in J_i$．现在 $n\geqslant 3$，从而至少有一个 J_i 是素理想，为了记号的方便，假定 J_1 是素理想．考虑元素

$$y = b_1 + b_2 b_3 \cdots b_{n+1}.$$

因一切 $b_i\in B$ 且 B 在加法和乘法下封闭，所以 $y\in B$. 现在 $y\notin J_1$，否则 $b_2b_3\cdots b_{n+1}=y-b_1\in J_1$．因 J_1 是素理想，所以有某个 $b_i\in J_1$．这是一个矛盾，因为 $b_i\notin D_i\supseteq J_1$．如果 $i>1$ 且 $y\in J_i$，则因为 J_i 是理想，所以 $b_2b_3\cdots b_{n+1}\in J_i$，从而 $b_1=y-b_2b_3\cdots b_{n+1}\in J_i$，这是不可能的，因为 $b_1\notin D_1\supseteq J_i$．所以对一切 i，$y\notin J_i$，这和 $B\subseteq J_1\cup\cdots\cup J_{n+1}$ 矛盾．

（ii）命题假设给出 $B\subseteq I\cup P_1\cup\cdots\cup P_n$，从而（i）给出 $B\subseteq I$ 或 $B\subseteq P_i$．因 I 是 B 的真子集，所以第一种可能性不可能出现． ■

习题

6.1 （i）求$\mathbb{Z}$中所有的极大理想．

（ii）求$\mathbb{R}[x]$中所有的极大理想，即描述 (g) 是极大理想的那些 $g(x)\in\mathbb{R}[x]$.

（iii）求$\mathbb{C}[x]$中所有的极大理想．

6.2 设 I 是交换环 R 中的理想．如果 J^* 和 L^* 都是 R/I 中的理想，证明存在 R 中包含 I 的理想 J 和 L 使得 $J/I=J^*$，$L/I=L^*$ 且 $(J\cap L)/I=J^*\cap L^*$．由此推出，如果 $J^*\cap L^*=\{0\}$，则 $J\cap L=I$.

提示：用对应定理．

6.3 （i）举出交换环的一个例子，它有两个素理想 P 和 Q，而 $P\cap Q$ 不是素理想．

（ii）如果 $P_1\supseteq P_2\supseteq\cdots P_n\supseteq P_{n+1}\supseteq\cdots$ 是交换环 R 中素理想的递减序列，证明 $\bigcap_{n\geqslant 1} P_n$ 是素理想． 324

6.4 设 $f:A\to R$ 是环同态，其中 A 和 R 是非零交换环．举出 A 中的素理想 P 的一个例子使得 $f(P)$ 不是 R 中的素理想．

6.5 设 $f:A\to R$ 是环同态．如果 Q 是 R 中的素理想，证明 $f^{-1}(Q)$ 是 A 中的素理想．由此推出，如果 J/I 是 R/I 中的素理想，其中 $I\subseteq J\subseteq R$，则 J 是 R 中的素理想．

6.6 （i）设 k 是域，$a_1,\cdots,a_n\in k$. 证明 $(x_1-a_1,\cdots,x_n-a_n)$ 是 $k[x_1,\cdots,x_n]$ 中的极大理想．

（ii）证明：如果对某个 i 有 $x_i-b\in(x_1-a_1,\cdots,x_n-a_n)$，其中 $b\in k$，则 $b=a_i$.

（iii）证明由

$$\mu:(a_1,\cdots,a_n)\mapsto(x_1-a_1,\cdots,x_n-a_n)$$

给出的 $\mu:k^n\to\{k[x_1,\cdots,x_n]$ 中的极大理想$\}$ 是单射，并举出域 k 的一个例子使得 μ 不是满射．

6.7 证明：如果 P 是交换环 R 中的素理想，又如果有某个 $r\in R$ 和 $n\geqslant 1$ 使得 $r^n\in P$，则 $r\in P$.

6.8 证明$\mathbb{Q}[x,y,z]$中的理想(x^2-2,y^2+1,z)是真理想．

6.9 （i）交换环 R 的一个非空子集 S 称为**乘法封闭的**，如果 $0\notin S$ 且对任意 $s,s'\in S$ 有 $ss'\in S$. 证明：如果理想 J 在满足性质 $J\cap S=\varnothing$ 的一切理想中极大，则 J 是素理想．（习题 6.48 中用佐恩引理证明了

这种理想的存在性.)

(ii) 设 S 是交换环 R 的乘法封闭子集，并假设有一个理想 I 满足 $I\cap S=\varnothing$. 如果理想 P 在满足性质 $I\subseteq P$ 和 $P\cap S=\varnothing$ 的一切理想中极大，证明 P 是素理想.

6.10 (i) 如果 I 和 J 都是交换环 R 中的理想，定义

$$IJ=\{一切有限和\sum_{\ell} a_\ell b_\ell : a_\ell\in I 和 b_\ell\in J\}.$$

证明 IJ 是 R 的理想且 $IJ\subseteq I\cap J$.

(ii) 如果 $I=(2)=J$ 是 $\mathbb{Z}$ 中偶整数的理想，证明 $I^2=IJ\subsetneq I\cap J=I$.

(iii) 设 P 是素理想，$Q_1,\cdots,Q_r$ 是理想. 证明：如果 $Q_1\cap\cdots\cap Q_r\subseteq P$，则有某个 i 使得 $Q_i\subseteq P$.

6.11 设 I 和 J 是交换环 R 中的理想.

(i) 证明由 $\varphi: r\mapsto(r+I,r+J)$ 给出的映射 $\varphi: R/(I\cap J)\to R/I\times R/J$ 是单射.

(ii) 如果 $I+J=R$，则称 I 和 J **互素**. 证明：如果 I 和 J 互素，则 (i) 中的环同态 $\varphi: R/(I\cap J)\to R/I\times R/J$ 是满射.

提示：如果 I 和 J 互素，则存在 $a\in I$ 和 $b\in J$ 使得 $1=a+b$. 如果 $r,r'\in R$，证明 $(d+I,d+J)=(r+I,r'+J)\in R/I\times R/J$，其中 $d=r'a+rb$.

(iii) 推广**孙子剩余定理**如下. 设 R 是交换环，并设 $I_1,\cdots,I_n$ 是两两互素的理想，即对一切 $i\neq j$，I_i 和 I_j 互素. 证明：如果 $a_1,\cdots,a_n\in R$，则存在 $r\in R$ 使得对一切 i 有 $r+I_i=a_i+I_i$.

6.12 如果 I 和 J 是交换环 R 中互素的理想，证明

325

$$I\cap J=IJ.$$

6.13 如果 I 是交换环 R 中的理想，并设 S 是 R 的子集，定义**冒号理想**[⊖]为

$$(I:S)=\{r\in R: rs\in I, 对所有 s\in S\}.$$

(i) 证明 $(I:S)$ 是理想.

(ii) 如果 $J=(S)$ 是由 S 生成的理想，证明 $(I:S)=(I:J)$.

(iii) 设 R 是整环，且 $a,b\in R$，其中 $b\neq 0$. 如果 $I=(ab)$，$J=(b)$，证明 $(I:J)=(a)$.

6.14 (i) 设 I 和 J 是交换环 R 中的理想. 证明 $I\subseteq(I:J)$ 和 $J(I:J)\subseteq I$.

(ii) 证明：如果 $I=Q_1\cap\cdots\cap Q_r$，则

$$(I:J)=(Q_1:J)\cap\cdots\cap(Q_r:J).$$

(iii) 如果 I 是交换环 R 中的理想，且 $J=J_1+\cdots+J_n$ 是理想的和，证明

$$(I:J)=(I:J_1)\cap\cdots\cap(I:J_n).$$

6.15 **布尔环**是指对一切 $a\in R$ 满足 $a^2=a$ 的交换环 R. 证明布尔环中的每个素理想都是极大理想.(见习题 8.21.)

提示：什么时候布尔环是整环？

6.16 交换环 R 称为**局部环**，如果它有唯一的极大理想.

(i) 如果 p 是素数，证明 **p-进位分数**的环

$$\mathbb{Z}_{(p)}=\{a/b\in\mathbb{Q}: p\nmid b\}$$

是局部环.

(ii) 如果 R 是有唯一极大理想 m 的局部环，证明 $a\in R$ 是单位当且仅当 $a\notin m$.

提示：可以假定交换环中的每个非单位在某个极大理想中(该结果是用佐恩引理证明的).

⊖ 这个理想也称为理想商.

6.2 唯一因子分解整环

我们已经证明了$\mathbb{Z}$和$k[x]$中的唯一因子分解定理，其中k是域．现在要证明一个普遍的结果：每个PID都有唯一因子分解定理．然后证明高斯的一个定理：如果R有唯一因子分解，则$R[x]$也有．一个推论是域k上的一切多元多项式的环$k[x_1,\cdots,x_n]$中有唯一因子分解．随后立刻导出任两个多元多项式有gcd.

我们先推广某些早先的定义．

326

定义 称交换环R中的元素a和b是**相伴**的，如果存在单位$u\in R$使得$b=ua$.

例如，$\mathbb{Z}$中的单位是±1，所以整数m的相伴元素只有$\pm m$；$k[x]$中的单位是非零常数，其中k是域，所以多项式$f(x)\in k[x]$的相伴元素只有多项式$uf(x)$，其中$u\in k$且$u\neq0$. $\mathbb{Z}[x]$中的单位只有±1（见习题6.19），所以多项式$f(x)\in\mathbb{Z}[x]$的相伴元素只有$\pm f(x)$.

在任一交换环R中，相伴元素a和b生成同一主理想，如果R不是整环，逆命题可能不成立．

命题6.15 设R是整环且a，$b\in R$.

（i）$a\mid b$且$b\mid a$当且仅当a和b是相伴的．

（ii）主理想(a)和(b)相等当且仅当a和b是相伴的．

证明 （i）如果$a\mid b$且$b\mid a$，则有r，$s\in R$使得$b=ra$和$a=sb$，从而$b=ra=rsb$. 如果$b=0$，则$a=0$（因为$b\mid a$）；如果$b\neq0$，则可以消去它（R是整环）得到$1=rs$. 因此r和s是单位，从而a和b是相伴的．逆命题显然成立．

（ii）如果$(a)=(b)$，则$a\in(b)$，因此有某个$r\in R$使得$a=rb$，从而$b\mid a$. 同样，$b\in(a)$蕴涵$a\mid b$，于是（i）证明a和b是相伴的．

反之，如果$a=ub$，其中u是单位，则$a\in(b)$且$(a)\subseteq(b)$. 同样，$b=u^{-1}a$蕴涵$(b)\subseteq(a)$，所以$(a)=(b)$. ■

回忆整环R中的元素p是不可约的，如果它既不是0也不是单位，而且它的因子只有单位或p的相伴元素．例如，$\mathbb{Z}$中不可约元素是数$\pm p$，其中p是素数．$k[x]$中的不可约元素（其中k是域）是不可约多项式$p(x)$，即$\deg(p)\geqslant1$且$p(x)$没有因式分解$p(x)=f(x)g(x)$，其中$\deg(f)<\deg(p)$和$\deg(g)<\deg(p)$．当R不是域时，不可约多项式的这个特征没有在环$R[x]$中保持下来．例如在$\mathbb{Z}[x]$中，多项式$f(x)=2x+2$不能够分解成两个次数都低于$\deg(f)=1$的多项式，但是$f(x)$不是不可约的，因为在因式分解$2x+2=2(x+1)$中，2和$x+1$两者都不是单位．

系6.16 如果R是PID，且$p\in R$是不可约的，则(p)是素理想．

证明 令I是一个理想满足$(p)\subseteq I$. 因R是PID，有某个$q\in R$使得$I=(q)$. 因此$p\in(q)$，从而有某个$r\in R$使得$p=rq$. p的不可约性说q或者是p的相伴，或者是单位．第一种情形，根据命题6.15，$(p)=(q)$；第二种情形，$(q)=R$. 由此，(p)是极大理想，因此根据系6.8，(p)是素理想． ■

下面是我们一直在探索的定义．

327

定义 整环R称为**唯一因子分解整环**（UFD），如果

（i）每个既不是0也不是单位的$r\in R$都是不可约元素的乘积[⊖]；

（ii）如果$up_1\cdots p_m=vq_1\cdots q_m$，其中$u$，$v$是单位，所有$p_i$和$q_j$都是不可约元素，则$m=n$，

⊖ 为避免句子太长，我们允许一个不可约元素的乘积只有一个因子，即把一个不可约元素也看作不可约元素的乘积．

并存在置换 $\sigma\in S_n$ 使得对一切 i，p_i 和 $q_{\sigma(i)}$ 相伴．

当我们证明Z 和 $k[x]$（其中 k 是域）有分解为不可约元素乘积的唯一因子分解时，并没有提到相伴，因为在每种情形中，总是选取中意的那个相伴元素来代替不可约元素．在Z 中，选取正不可约元素（即素数）；在 $k[x]$ 中，选取首一不可约多项式．例如，读者应该知道“Z 是一个 UFD”这样的陈述就是算术基本定理的重述．

命题 6.17 设 R 是整环，其中每个既不是 0 也不是单位的 $r\in R$ 都是不可约元素的乘积，则 R 是 UFD 当且仅当对每个不可约元素 $p\in R$，(p) 是 R 中的素理想．⊖

证明 假定 R 是 UFD. 如果 a，$b\in R$ 且 $ab\in(p)$，则有 $r\in R$ 使得

$$ab = rp.$$

把 a，b 和 r 的每一个都分解为不可约元素的乘积，根据唯一因子分解，等式的左端必含有 p 的相伴．这个相伴元素作为 a 或 b 的因子产生，因此 $a\in(p)$ 或 $b\in(p)$．

逆命题的证明仅仅是算术基本定理的证明的修改．假定

$$up_1\cdots p_m = vq_1\cdots q_n,$$

其中 p_i 和 q_j 是不可约元素，u，v 是单位．对 $\max\{m,n\}\geqslant 1$用归纳法证明 $n=m$ 且各个 q 可以重新标号使得对一切 i，q_i 和 p_i 相伴．如果 $\max\{m,n\}=1$，则 $up_1=vq_1$，$up_1=v$ 或 $u=vq_1$. 后两种情形不可能发生，因为不可约元素不是单位，因此基础步为真．关于归纳步，给出的等式表明 $p_1\mid q_1\cdots q_n$. 根据假设 (p_1) 是素理想（类似于欧几里得引理），因此存在某个 q_j 使得 $p_1\mid q_j$. 而 q_j 是不可约元素，除了单位和相伴外没有其他的因子，所以 q_j 和 p_1 相伴：有某个单位 u 使得 $q_j=up_1$. 两端消去 p_1 得 $p_2\cdots p_m=uq_1\cdots\hat{q}_j\cdots q_n$. 由归纳假设，$m-1=n-1$（从而 $m=n$），且经过重新标号，对一切 i 有 q_i 和 p_i 相伴． ■

我们已经给出的Z 和 $k[x]$（其中 k 是域）是 UFD 的证明涉及带余除法，因此，不难将其推广以证明每个欧几里得环是 UFD. 我们现在证明每个 PID 事实上都是一个 UFD，证明用到了一个新概念：理想的链．

328

引理 6.18 （i）如果 R 是交换环且

$$I_1\subseteq I_2\subseteq\cdots\subseteq I_n\subseteq I_{n+1}\subseteq\cdots$$

是 R 中理想的升链，则 $J=\bigcup_{n\geqslant 1} I_n$ 是 R 中的理想．

（ii）如果 R 是 PID，则不存在理想的无限严格升链

$$I_1\subsetneq I_2\subsetneq\cdots\subsetneq I_n\subsetneq I_{n+1}\subsetneq\cdots.$$

（iii）设 R 是 PID. 如果 $r\in R$ 既不是 0 也不是单位，则 r 是不可约元素的乘积．

证明 （i）我们断言 J 是理想．如果 $a\in J$，则有某个 n 使得 $a\in I_n$. 如果 $r\in R$，则因为 I_n 是理想，有 $ra\in I_n$，因此 $ra\in J$. 如果 a，$b\in J$，则存在理想 I_n 和 I_m 使得 $a\in I_n$ 和 $b\in I_m$. 因链是递升的，可以假定 $I_n\subseteq I_m$，从而 a，$b\in I_m$. 因为 I_m 是理想，所以 $a+b\in I_m$，从而 $a+b\in J$. 因此 J 是理想．

（ii）如果相反，存在一个无限严格升链，则定义 $J=\bigcup_{n\geqslant 1} I_n$．根据（i），$J$ 是理想．因 R 是 PID，所以有某个 $d\in J$ 使得 $J=(d)$. 现在对某个 nd 取自 J，所以必在某个 I_n 中，因此

⊖ (p) 是非零素理想的元素 p 常称为素元素. 这种元素具有性质：$p|ab$ 蕴涵 $p|a$ 或 $p|b$.

$$J = (d) \subseteq I_n \subsetneq I_{n+1} \subseteq J,$$

这是一个矛盾.

(iii) 元素 $a \in R$ 的一个因子 r 叫做 a 的真因子，如果 r 既不是单位也不是 a 的相伴. 如果 r 是 a 的因子，则 $(a) \subseteq (r)$；如果 r 是 a 的真因子，则 $(a) \subsetneq (r)$，这是因为如果不等式不是严格的，则 $(a) = (r)$，根据命题 6.15，这使得 a 和 r 相伴.

把非零非单位的 $a \in R$ 叫做好的，如果它是不可约元素的乘积，否则把它叫做坏的. 我们必须证明没有坏元素. 如果 a 是坏的，它就不是不可约的，从而 $a=rs$，其中 r 和 s 两者都是真因子. 但好元素的乘积还是好元素，所以至少一个因子是坏的，比如 r. 第一段证明了 $(a) \subsetneq (r)$. 由此，用归纳法可得坏元素的一个序列 $a_1=a, a_2=r, a_3, \cdots, a_n, \cdots$，其中每个 a_{n+1} 是 a_n 的真因子，这个序列产生一个严格升链

$$(a_1) \subsetneq (a_2) \subsetneq \cdots \subsetneq (a_n) \subsetneq (a_{n+1}) \subsetneq \cdots,$$

与本引理的 (ii) 矛盾. ■

定理 6.19 如果 R 是 PID，则 R 是 UFD. 特别地，每个欧几里得环都是 UFD.

证明 依据上面两个结果，只要证明当 p 是不可约元素时，(p) 是素理想. 因 R 是 PID，命题 6.16 表明 (p) 是素理想. ■

329

gcd 的概念可以在任意交换环 R 中定义. 例 6.21 证明存在这样的整环 R，它包含一对没有 gcd 的元素. 如果 $a_1, \cdots, a_n \in R$，则 $a_1, \cdots, a_n$ 的公因子是满足对一切 i 有 $c \mid a_i$ 的元素 $c \in R$. $a_1, \cdots, a_n$ 的最大公因子或 gcd 是公因子 d，满足对每个公因子 c 有 $c \mid d$. 甚至在 $\mathbb{Z}$ 和 $k[x]$ 这种熟悉的例子中，除非利用额外的条件，否则 gcd 就不唯一. 例如在 $k[x]$ 中，其中 k 是域，我们利用了非零 gcd 是首一多项式的条件. 然而在一般的 PID 中，元素未必有合适的相伴.

如果 R 是整环，易知如果 d 和 d' 都是元素 $a_1, \cdots, a_n$ 的 gcd，则 $d \mid d'$ 且 $d' \mid d$. 由此，根据命题 6.15，d 和 d' 相伴，因此 $(d) = (d')$. 于是，gcd 虽然不唯一，但它们生成相同的主理想.

命题 1.17 中的思想可以继续证明 UFD 中存在 gcd.

命题 6.20 如果 R 是 UFD，则 R 中元素的任意一个有限集合 $a_1, \cdots, a_n$ 存在 gcd.

证明 只要证明两个元素 a 和 b 存在 gcd，一般结果可对元素个数用归纳法得到.

存在单位 u 和 v 以及不同的不可约元素 $p_1, \cdots, p_t$ 使得

$$a = up_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$$

和

$$b = vp_1^{f_1} p_2^{f_2} \cdots p_t^{f_t},$$

其中对一切 i，$e_i \geqslant 0$ 和 $f_i \geqslant 0$. 易知，如果 $c \mid a$，则把 c 分解为不可约元素的因子分解是 $c = wp_1^{g_1} p_2^{g_2} \cdots p_t^{g_t}$，其中 w 是单位，且对一切 i，$0 \leqslant g_i \leqslant e_i$. 于是，$c$ 是 a 和 b 的公因子当且仅当对一切 i，$g_i \leqslant m_i$，其中

$$m_i = \min\{e_i, f_i\}.$$

显然 $p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$ 是 a 和 b 的 gcd. ■

不难看出，如果 $a_i = u_i p_1^{e_{i1}} p_2^{e_{i2}} \cdots p_e^{e_{it}}$，其中 $e_{ij} \geqslant 0$，u_i 是单位，$i=1, \cdots, n$，则

$$d = p_1^{\mu_1} p_2^{\mu_2} \cdots p_t^{\mu_t}$$

是 $a_1, \cdots, a_n$ 的 gcd，其中 $\mu_j = \min\{e_{1j}, e_{2j}, \cdots, e_{nj}\}$.

我们告诫读者我们没有证明元素 $a_1, \cdots, a_n$ 的 gcd 是它们的线性组合，事实上，这有可能不成

立（见习题 6.21）.

例 6.21 设 k 是域，并设 R 是 $k[x]$ 的子环，它由一切没有线性项的多项式 $f(x) \in k[x]$ 组成；即 $f(x) = a_0 + a_2x^2 + \cdots + a_nx^n$. 习题 3.60 中我们证明了 x^5 和 x^6 在 R 中没有 gcd. 现在由命题 6.20 可知 R 不是 UFD.［整环不是 UFD 的另一例在习题6.31(ⅱ)中给出.］ ■

330

定义 称 UFD 中的元素 $a_1, \cdots, a_n$ **互素**，如果它们的 gcd 是单位；即 $a_1, \cdots, a_n$ 的每个公因子都是单位.

我们现在要证明如果 R 是 UFD，则 $R[x]$ 也是. 回忆习题 3.21：如果 R 是整环，则 $R[x]$ 中的单位也是 R 中的单位.

定义 设 R 是 UFD，多项式 $f(x) = a_nx^n + \cdots + a_1x + a_0 \in R[x]$ 称为**本原的**，如果它的系数互素，即 $a_n, \cdots, a_1, a_0$ 的公因子只有单位.

当然，每个首一多项式是本原多项式. 注意，如果 $f(x)$ 不是本原的，则存在不可约元素 $q \in R$ 整除它的每个系数：如果 gcd 是一个非单位 d，则 q 取为 d 的任一不可约因子即可.

例 6.22 我们现在证明，对于一个 UFD R，每个正次数不可约多项式 $p(x) \in R[x]$ 都是本原的. 如果不是，则存在不可约元素 $q \in R$ 使得 $p(x) = qg(x)$. 注意，因为 $q \in R$，所以 $\deg(q) = 0$. 因 $p(x)$ 是不可约的，它只有单位和相伴多项式是它的因子，因此 q 必是 $p(x)$ 的相伴. 但 $R[x]$ 中的每个单位的次数都为 0［即都是常数（因为 $uv=1$ 蕴涵 $\deg(u) + \deg(v) = \deg(1) = 0$），因此，$R[x]$ 中的相伴多项式都有相同的次数. 所以 q 不是 $p(x)$ 的相伴，因为 $p(x)$ 的相伴有正次数，由此可知 $p(x)$ 是本原多项式. ■

我们先给出一个技术性的引理.

引理 6.23（高斯引理） *如果 R 是 UFD 且 $f(x), g(x) \in R[x]$ 两者都是本原多项式，则它们的积 $f(x)g(x)$ 也是本原多项式.*

证明 如果 $\pi: R \to R/(p)$ 是自然映射 $\pi: a \mapsto a + (p)$，则命题 3.48 表明把多项式的每个系数 c 换成 $\pi(c)$ 的函数 $\tilde{\pi}: R[x] \to (R/(p))[x]$ 是环同态. 如果多项式 $h(x) \in R[x]$ 不是本原的，则存在不可约元素 p 使得 $\tilde{\pi}(h)$ 的一切系数在 $R/(p)$ 中为 0，即在 $(R/(p))[x]$ 中 $\tilde{\pi}(h) = 0$. 由此，如果乘积 $f(x)g(x)$ 不是本原的，则存在某个不可约元素 p 使得在 $(R/(p))[x]$ 中有 $0 = \tilde{\pi}(fg) = \tilde{\pi}(f)\tilde{\pi}(g)$. 因 (p) 是素理想，$R/(p)$ 是整环，从而 $(R/(p))[x]$ 也是整环. 但因为 f 和 g 都是本原的，所以在 $(R/(p))[x]$ 中 $\tilde{\pi}(f)$ 和 $\tilde{\pi}(g)$ 都不是 0，这与 $(R/(p))[x]$ 是整环矛盾. ■

引理 6.24 *设 R 是 UFD，并设 $Q = \mathrm{Frac}(R)$ 和 $f(x) \in Q[x]$ 非零.*

（ⅰ）存在因式分解

$$f(x) = c(f)f^*(x),$$

其中 $c(f) \in Q$，$f^*(x) \in R[x]$ 是本原多项式. 这个因式分解在下列意义下唯一：如果 $f(x) = qg^*(x)$，其中 $q \in Q$，$g^*(x) \in R[x]$ 是本原的，则存在单位 $w \in R$ 使得 $q = wc(f)$ 和 $g^*(x) = w^{-1}f^*(x)$.

331

（ⅱ）如果 $f(x), g(x) \in R[x]$，则 $c(fg)$ 和 $c(f)c(g)$ 在 R 中相伴，$(fg)^*$ 和 f^*g^* 在 $R[x]$ 中相伴.

（ⅲ）设 $f(x) \in Q[x]$ 有因式分解 $f(x) = qg^*(x)$，其中 $q \in Q$，$g^*(x) \in R[x]$ 是本原的，则 $f(x) \in R[x]$ 当且仅当 $q \in R$.

（ⅳ）设 $g^*(x), f(x) \in R[x]$. 如果 $g^*(x)$ 是本原的且 $g^*(x) \mid bf(x)$，其中 $b \in R$ 且 $b \neq 0$，则

$g^*(x) \mid f(x)$.

证明 （ⅰ）通分，存在 $b \in R$ 使得 $bf(x) \in R[x]$. 如果 d 是 $bf(x)$ 系数的 gcd，则 $(b/d)f(x) \in R[x]$ 是本原多项式. 如果定义 $c(f) = d/b$ 和 $f^*(x) = (c(f))^{-1}f(x)$，则 $f^*(x)$ 是本原的且 $f(x) = c(f)f^*(x)$.

为证明唯一性，假设 $c(f)f^*(x) = f(x) = qg^*(x)$，其中 $c(f), q \in Q$，$f^*(x), g^*(x) \in R[x]$ 是本原的. 习题 6.17 允许我们把 $q/c(f)$ 写作既约形式：$q/c(f) = u/v$，其中 u, v 是 R 中的互素元素. 在 $R[x]$ 中等式 $vf^*(x) = ug^*(x)$ 成立，由同次项系数相等可知 v 是 $ug^*(x)$ 的每个系数的公因子. 因 u 和 v 互素，习题6.18(ⅰ)给出 v 是 $g^*(x)$ 的系数的公因子. 而 $g^*(x)$ 是本原的，因此 v 是单位. 类似的推理证明 u 也是单位. 所以 $q/c(f) = u/v$ 是 R 中的单位，把它叫做 w，于是正如所要的有 $wc(f) = q$ 和 $f^*(x) = wg^*(x)$.

（ⅱ）$f(x)g(x)$ 在 $R[x]$ 中有两个因式分解：$f(x)g(x) = c(fg)(f(x)g(x))^*$ 和 $f(x)g(x) = c(f)f^*(x)c(g)g^*(x) = c(f)c(g)f^*(x)g^*(x)$. 因本原多项式的积还是本原多项式，这两个分解都是（ⅰ）中的那种分解，而（ⅰ）中声称的唯一性给出 $c(fg)$ 是 $c(f)c(g)$ 的相伴，$(fg)^*$ 是 f^*g^* 的相伴.

（ⅲ）如果 $q \in R$，则显然有 $f(x) = qg^*(x) \in R[x]$. 反之，如果 $f(x) \in R[x]$，则没有必要通分，从而 $c(f) = d \in R$，其中 d 是 $f(x)$ 系数的公因子. 于是 $f(x) = df^*(x)$. 根据唯一性，存在单位 $w \in R$ 使得 $q = wd \in R$.

（ⅳ）因 $bf = hg^*$，有 $bc(f)f^* = c(h)h^*g^* = c(h)(hg)^*$. 根据唯一性，$f^*$，$(hg)^*$ 和 h^*g^* 都是相伴的，因此 $g^* \mid f^*$. 而 $f = c(f)f^*$，所以 $g^* \mid f$. ■

定义 设 R 是 UFD 且 $Q = \mathrm{Frac}(R)$. 如果 $f(x) \in Q[x]$，则有因式分解 $f(x) = c(f)f^*(x)$，其中 $c(f) \in Q$，$f^*(x) \in R[x]$ 是本原的. 则 $c(f)$ 称为 $f(x)$ 的**容度**，$f^*(x)$ 称为 $f(x)$ 的**相伴本原多项式**.

依据引理6.24(ⅰ)，$c(f)$ 和 $f^*(x)$ 两者本质上都是唯一的，只不过相差 R 中的一个单位.

定理 6.25（高斯） 如果 R 是 UFD，则 $R[x]$ 也是 UFD.

证明 先对 $\deg(f)$ 用归纳法证明每个非零、非单位的 $f(x) \in R[x]$ 都是不可约多项式的积. 如果 $\deg(f) = 0$，则 $f(x)$ 是常数，因此在 R 中. 因 R 是 UFD，所以 f 是不可约多项式的乘积. 如果 $\deg(f) > 0$，则 $f(x) = c(f)f^*(x)$，其中 $c(f) \in R$，$f^*(x)$ 是本原多项式. 现在，根据基础步，$c(f)$ 或者是单位，或者是不可约元素的积. 如果 $f^*(x)$ 是不可约的，证明已经完成. 否则 $f^*(x) = g(x)h(x)$，其中 g 和 h 都不是单位. 然而 $f^*(x)$ 是本原的，因此 g 和 h 都不是常数，所以它们的次数都低于 $\deg(f^*) = \deg(f)$，根据归纳假设两者都是不可约多项式的积. 332

现在应用命题 6.17：如果对每个不可约的 $p(x) \in R[x]$，$(p(x))$ 是素理想，即如果 $p \mid fg$，那么 $p \mid f$ 或 $p \mid g$，则 $R[x]$ 是 UFD. 假定 $p(x) \nmid f(x)$.

第（ⅰ）种情形. 假设 $\deg(p) = 0$. 记

$$f(x) = c(f)f^*(x) \text{ 和 } g(x) = c(g)g^*(x),$$

其中 $c(f), c(g) \in R$，$f^*(x), g^*(x)$ 是本原的. 现在 $p \mid fg$，从而

$$p \mid c(f)c(g)f^*(x)g^*(x).$$

因 $f^*(x)g^*(x)$ 是本原的，引理6.24(ⅱ)说 $c(f)c(g)$ 是 $c(fg)$ 的相伴. 然而，如果 $p \mid f(x)g(x)$，则 p 整除 fg 的每个系数，即 p 是 fg 的一切系数的公因子，因此在 R 中，注意 R 是 UFD，p 整除相伴

的 $c(fg)$ 和 $c(f)c(g)$．而命题 6.17 说 (p) 是 R 中的素理想，因此 $p \mid c(f)$ 或 $p \mid c(g)$．如果 $p \mid c(f)$，则 p 整除 $c(f)f^*(x) = f(x)$，产生矛盾．所以 $p \mid c(g)$，因此正如所要的 $p \mid g(x)$．

第（ⅱ）种情形．假设 $\deg(p) > 0$．令

$$(p,f) = \{s(x)p(x) + t(x)f(x) : s(x),t(x) \in R[x]\};$$

当然，(p,f) 是包含 $p(x)$ 和 $f(x)$ 的理想．选取 $m(x) \in (p,f)$ 具有极小次数．如果 $Q = \mathrm{Frac}(R)$ 是 R 的分式域，则 $Q[x]$ 中的带余除法给出多项式 $q'(x), r'(x) \in Q[x]$ 使得

$$f(x) = m(x)q'(x) + r'(x),$$

其中 $r'(x) = 0$ 或 $\deg(r') < \deg(m)$．通分，存在多项式 $q(x), r(x) \in R[x]$ 和常数 $b \in R$ 使得

$$bf(x) = q(x)m(x) + r(x),$$

其中 $r(x) = 0$ 或 $\deg(r) < \deg(m)$．因 $m \in (p,f)$，存在多项式 $s(x),t(x) \in R[x]$ 使得 $m(x) = s(x)p(x) + t(x)f(x)$，因此 $r = bf - qm \in (p,f)$．由于 m 在 (p,f) 中有极小次数，因此必有 $r = 0$；即 $bf(x) = m(x)q(x)$，从而 $bf(x) = c(m)m^*(x)q(x)$．但 $m^*(x)$ 是本原的，且 $m^*(x) \mid bf(x)$，所以根据引理 6.24(ⅳ)，$m^*(x) \mid f(x)$．把 $f(x)$ 换成 $p(x)$ 作类似的推理（即从等式 $b''p(x) = q''(x)m(x) + r''(x)$ 开始，其中 b'' 是某个常数），给出 $m^*(x) \mid p(x)$．因 $p(x)$ 是不可约的，因此它的因子只有单位和相伴．如果 $m^*(x)$ 是 $p(x)$ 的相伴，则 $p(x) \mid f(x)$（因为 $p(x) \mid m^*(x) \mid f(x)$），与假设矛盾．因此 $m^*(x)$ 必是一个单位，即 $m(x) = c(m) \in R$，从而 (p,f) 包含非零常数 $c(m)$．现在 $c(m) = sp + tf$，从而

333

$$c(m)g(x) = s(x)p(x)g(x) + t(x)f(x)g(x).$$

因 $p(x) \mid f(x)g(x)$，所以有 $p(x) \mid c(m)g(x)$．但因 $p(x)$ 是不可约的，所以根据例 6.22，$p(x)$ 是本原的，由此引理6.24(ⅳ)给出 $p(x) \mid g(x)$． ■

系 6.26 如果 k 是域，则 $k[x_1,\cdots,x_n]$ 是 UFD.

证明 对 $n \geq 1$ 用归纳法证明．在第 3 章中我们已经证明一元多项式环 $k[x_1]$ 是 UFD. 关于归纳步，回忆 $k[x_1,\cdots,x_n,x_{n+1}] = R[x_{n+1}]$，其中 $R = k[x_1,\cdots,x_n]$．根据归纳假设，R 是 UFD，从而根据定理 6.25，$R[x_{n+1}]$ 也是 UFD. ■

命题 6.20 表明，如果 k 是域，则 $k[x_1,\cdots,x_n]$ 中存在 gcd.

系 6.27（高斯） 设 R 是 UFD，$Q = \mathrm{Frac}(R)$，$f(x) \in R[x]$．如果在 $Q[x]$ 中有

$$f(x) = G(x)H(x),$$

则在 $R[x]$ 中有因式分解

$$f(x) = g(x)h(x),$$

其中 $\deg(g) = \deg(G)$ 和 $\deg(h) = \deg(H)$．事实上，$G(x)$ 是 $g(x)$ 的常数倍，$H(x)$ 是 $h(x)$ 的常数倍．所以，如果 $f(x)$ 在 $R[x]$ 中不能分解为次数较小的多项式，则 $f(x)$ 在 $Q[x]$ 中是不可约的．

证明 根据引理6.24(ⅰ)，在 $Q[x]$ 中的因式分解 $f(x) = G(x)H(x)$ 给出 $q,q' \in Q$ 使得在 $Q[x]$ 中

$$f(x) = qG^*(x)q'H^*(x),$$

其中 $G^*(x), H^*(x) \in R[x]$ 是本原多项式．而根据高斯引理，$G^*(x)H^*(x)$ 也是本原的．因 $f(x) \in R[x]$，运用引理6.24(ⅲ)，等式 $f(x) = qq'[G^*(x)H^*(x)]$ 迫使 $qq' \in R$．所以，$qq'G^*(x) \in R[x]$，从而 $f(x)$ 在 $R[x]$ 中的一个因式分解是 $f(x) = [qq'G^*(x)]H^*(x)$． ■

$R = \mathbb{Z}$ 和 $Q = \mathbb{Q}$ 的特殊情形当然是重要的．

例 6.28 我们断言 $f(x,y)=x^2+y^2-1\in k[x,y]$ 是不可约的，其中 k 是域．记 $Q=k(y)=\mathrm{Frac}(k[y])$，并看作 $f(x,y)\in Q[x]$．现在二次多项式 $g(x)=x^2+(y^2-1)$ 在 $Q[x]$ 中不可约当且仅当它没有根在 $Q=k(y)$ 中，根据习题 3.34，确实如此．

因为 x^2+y^2-1 是由不可约多项式生成的，因此由命题 6.17，它是素理想． ■

回忆一个复数是代数整数如果它是 $\mathbb{Z}[x]$ 中的一个首一多项式的根．每个代数整数有一个不可约多项式相伴于它．

334

系 6.29 如果 α 是一个代数整数，则 $\mathrm{irr}(\alpha,\mathbb{Q})$ 在 $\mathbb{Z}[x]$ 中．

证明 设 $p(x)\in\mathbb{Z}[x]$ 是以 α 为根的次数最小的首一多项式．如果在 $\mathbb{Q}[x]$ 中有 $p(x)=G(x)H(x)$，其中 $\deg(G)<\deg(p)$ 和 $\deg(H)<\deg(p)$，则 α 不是 $G(x)$ 的根就是 $H(x)$ 的根．根据高斯引理，在 $\mathbb{Z}[x]$ 中有因式分解 $p(x)=g(x)f(x)$，其中 $\deg(g)=\deg(G)$ 和 $\deg(h)=\deg(H)$，事实上，存在有理数 c 和 d 使得 $g(x)=cG(x)$ 和 $h(x)=dH(x)$．如果 a 是 $g(x)$ 的首项系数，b 是 $h(x)$ 的首项系数，则因 $p(x)$ 是首一的，$ab=1$．所以由 $a,b\in\mathbb{Z}$，我们可假定 $a=1=b$，即假定 $g(x)$ 和 $h(x)$ 两者都是首一的．因 α 是 $g(x)$ 或 $h(x)$ 的根，这和 $p(x)$ 是 $\mathbb{Z}[x]$ 中以 α 为根次数最小的首一多项式矛盾．因 $\mathrm{irr}(\alpha,\mathbb{Q})$ 是 $\mathbb{Q}[x]$ 中唯一的以 α 为根的首一不可约多项式，所以 $p(x)=\mathrm{irr}(\alpha,\mathbb{Q})$． ■

定义 如果 α 是代数整数，它的**极小多项式**是指 $\mathbb{Z}[x]$ 中以 α 为根次数最小的首一多项式．

系 6.29 表明每个代数整数 α 都有唯一的极小多项式 $m(x)\in\mathbb{Z}[x]$，即 $m(x)=\mathrm{irr}(\alpha,\mathbb{Q})$，且 $m(x)$ 在 $\mathbb{Q}[x]$ 中不可约．

注 我们定义 α 的（代数）**共轭**为 $\mathrm{irr}(\alpha,\mathbb{Q})$ 的根，并定义 α 的**范数**为 α 的共轭之积的绝对值．当然，α 的范数正是 $\mathrm{irr}(\alpha,\mathbb{Q})$ 的常数项的绝对值，因此它是一个（常规）整数．范数在代数数论中非常有用，我们已经在费马二平方和定理，即定理 3.66 的证明中看到过．在希尔伯特定理 90 的证明中也考虑过它们，在那里用来证明如果多项式 $f(x)\in k[x]$ 的伽罗瓦群是可解的，其中 k 有特征 0，则 $f(x)$ 运用根式可解．

下一判别法用了整数 mod$p$．

定理 6.30 设 $f(x)=a_0+a_1x+a_2x^2+\cdots+x^n\in\mathbb{Z}[x]$ 是首一的，并设 p 是素数．如果 $f(x)$ mod$p$ 不可约，即如果

$$\bar{f}(x)=[a_0]+[a_1]x+[a_2]x^2+\cdots+x^n\in\mathbb{F}_p[x]$$

是不可约的，则 $f(x)$ 在 $\mathbb{Q}[x]$ 中不可约．

证明 根据命题 3.48，自然映射 $\varphi:\mathbb{Z}\to\mathbb{F}_p$ 定义了一个同态 $\tilde{\varphi}:\mathbb{Z}[x]\to\mathbb{F}_p[x]$ 为

$$\tilde{\varphi}(b_0+b_1x+b_2x^2+\cdots)=[b_0]+[b_1]x+[b_2]x^2+\cdots;$$

即用 mod$p$ 约化所有系数．如果 $g(x)\in\mathbb{Z}[x]$，则记它的象 $\tilde{\varphi}(g(x))\in\mathbb{F}_p[x]$ 为 $\bar{g}(x)$．假设 $f(x)$ 在 $\mathbb{Z}[x]$ 中可分解，比如 $f(x)=g(x)h(x)$，其中 $\deg(g)<\deg(f)$ 和 $\deg(h)<\deg(f)$，当然，$\deg(f)=\deg(g)+\deg(h)$．现在因为 $\tilde{\varphi}$ 是环同态，从而 $\bar{f}(x)=\bar{g}(x)\bar{h}(x)$，因此 $\deg(\bar{f})=\deg(\bar{g})+\deg(\bar{h})$．因 $f(x)$ 是首一的，$\bar{f}(x)$ 也是首一的，所以 $\deg(\bar{f})=\deg(f)$．由此，$\bar{g}(x)$ 和 $\bar{h}(x)$ 的次数都小于 $\deg(\bar{f})$，与 $\bar{f}(x)$ 的不可约性矛盾．所以 $f(x)$ 在 $\mathbb{Z}[x]$ 中不可约，又根据高斯定理，即系 6.27，$f(x)$ 在 $\mathbb{Q}[x]$ 中不可约． ■

335

例 6.31 定理 6.30 的逆不成立．容易找到一个不可约多项式 $f(x)\in\mathbb{Z}[x]\subseteq\mathbb{Q}[x]$，使得 $f(x)$ 对某个素数 p，mod$p$ 可因式分解，但现在我们证明 $f(x)=x^4+1$ 是 $\mathbb{Z}[x]$ 中的不可约多项式，

它对每个素数 p，mod$p$ 可因式分解.

首先，$f(x)$ 在$\mathbb{Q}[x]$中不可约. 根据系 3.44，$f(x)$ 没有有理根，所以在$\mathbb{Q}[x]$中唯一可能的因式分解形如

$$x^4+1=(x^2+ax+b)(x^2-ax+c).$$

展开右端乘积，由同次项系数相等得

$$c+b-a^2=0$$
$$a(c-b)=0$$
$$bc=1.$$

第二个方程迫使 $a=0$ 或 $c=b$，由此立刻可以看到无论哪种情形都导出矛盾.

我们现在证明对一切素数 p，x^4+1 在$\mathbb{F}_p[x]$中不是不可约的. 如果 $p=2$，则 $x^4+1=(x+1)^4$，所以可以假定 p 是奇素数. 和在例1.21(ⅰ)中看到的一样，每个平方数和 0，1 或 4mod8 同余，因 p 是奇数，必有 $p^2\equiv 1 \bmod 8$. 所以 $|(\mathbb{F}_{p^2})^\times|=p^2-1$ 被 8 整除. 但 $(\mathbb{F}_{p^2})^\times$ 是循环群，根据引理 2.85，它有 8 阶（循环）子群. 由此，$\mathbb{F}_{p^2}$ 包含一切 8 次单位根，特别地，$\mathbb{F}_{p^2}$ 包含 x^4+1 的一切根. 因此 x^4+1 在$\mathbb{F}_p$上的分裂域 E_p 是$\mathbb{F}_{p^2}$，从而 $[E_p:\mathbb{F}_p]=2$. 但如果 x^4+1 在$\mathbb{F}_p[x]$中不可约，则由系 4.9，$4\mid[E_p:\mathbb{F}_p]$. 所以 x^4+1 对每个素数 p 在$\mathbb{F}_p[x]$中可因式分解. ■

定理 6.30 说，如果能够找到一个素数 p 使得 $\bar{f}(x)$ 在$\mathbb{F}_p[x]$中不可约，则 $f(x)$ 在$\mathbb{Q}[x]$中不可约. 在此之前，有限域$\mathbb{F}_p$是古怪的，它只是作为一种好奇的、人为的构造物出现的，现在$\mathbb{F}_p$的有限性是一种真正的好处，因为在$\mathbb{F}_p[x]$中任意给定次数的多项式只有有限个. 在例3.35(ⅰ)和3.35(ⅱ)中，我们列出了$\mathbb{F}_2$和$\mathbb{F}_3$上次数$\leqslant 3$的一切首一不可约多项式. 原则上，我们可以测试一个 n 次多项式在$\mathbb{F}_p[x]$中是否不可约，这可以通过看它的一切可能的因式分解来实现.

例 6.32 (ⅰ) 我们证明 $f(x)=x^4-5x^3+2x+3$ 是$\mathbb{Q}[x]$中的不可约多项式.

根据系 3.44，$f(x)$ 的有理根的候选者只有 1，-1，3，-3，读者可以验证它们都不是根. 因 $f(x)$ 是四次多项式，我们还不能下结论说 $f(x)$ 不可约，它也许是（不可约）二次多项式的乘积.

336

我们来试试定理 6.30 的判别法. 根据例3.35(ⅰ)，因 $\bar{f}(x)=x^4+x^3+1$ 在$\mathbb{F}_2[x]$中不可约，由此 $f(x)$ 在$\mathbb{Q}[x]$中不可约. [不必验证 $f(x)$ 没有有理根，$\bar{f}(x)$ 的不可约性足以导出 $f(x)$ 的不可约性.]

(ⅱ) 设 $\Phi_5(x)=x^4+x^3+x^2+x+1\in\mathbb{Q}[x]$.

在例3.35(ⅰ)中我们看到 $\bar{\Phi}_5(x)=x^4+x^3+x^2+x+1$ 在$\mathbb{F}_2[x]$中不可约，因此 $\Phi_5(x)$ 在$\mathbb{Q}[x]$中不可约. ■

回忆如果 n 是正整数，则 n 阶分圆多项式是

$$\Phi_n(x)=\prod(x-\zeta),$$

其中ζ遍历一切 n 次单位原根.

根据命题 1.37，对每个整数 $n\geqslant 1$，

$$x^n-1=\prod_{d\mid n}\Phi_d(x),$$

其中 d 遍历 n 的一切因数 d. 现在 $\Phi_1(x)=x-1$. 当 p 是素数时，

$$x^p-1=\Phi_1(x)\Phi_p(x)=(x-1)\Phi_p(x),$$

从而

$$\Phi_p(x)=(x^p-1)/(x-1)=x^{p-1}+x^{p-2}+\cdots+x+1.$$

和任意线性多项式一样，$\Phi_2(x)=x+1$ 在 $\mathbb{Q}[x]$ 中不可约；分圆多项式 $\Phi_3(x)=x^2+x+1$ 在 $\mathbb{Q}[x]$ 中不可约是因为它没有有理根；我们刚才已经知道 $\Phi_5(x)$ 在 $\mathbb{Q}[x]$ 中不可约．为证明对一切素数 p，$\Phi_p(x)$ 在 $\mathbb{Q}[x]$ 中不可约，我们介绍另一个不可约性的判别法．

引理 6.33 设 $g(x)\in\mathbb{Z}[x]$．如果存在 $c\in\mathbb{Z}$ 使得 $g(x+c)$ 在 $\mathbb{Z}[x]$ 中不可约，则 $g(x)$ 在 $\mathbb{Q}[x]$ 中不可约．

证明 根据习题 3.43，由 $f(x)\mapsto f(x+c)$ 给出的函数 $\varphi:\mathbb{Z}[x]\to\mathbb{Z}[x]$ 是同构．如果 $g(x)=s(x)t(x)$，则 $g(x+c)=\varphi(g(x))=\varphi(st)=\varphi(s)\varphi(t)$ 是一个不允许的分解．所以 $g(x)$ 在 $\mathbb{Z}[x]$ 中不可约，因此，根据高斯定理，即系 6.27，$g(x)$ 在 $\mathbb{Q}[x]$ 中不可约． ■

下一结果由艾森斯坦发现．下面的艾森斯坦准则的优美证明是 1969 年 R. Singer 的论文，见 Montgomery-Ralston，《Selected Papers in Algebra》．

定理 6.34（艾森斯坦准则） 设 R 是 UFD 且 $Q=\mathrm{Frac}(R)$，并设 $f(x)=a_0+a_1x+\cdots+a_nx^n\in R[x]$．如果存在不可约元素 $p\in R$ 使得对一切 $i<n$，$p\mid a_i$，但 $p\nmid a_n$ 和 $p^2\nmid a_0$，则 $f(x)$ 在 $Q[x]$ 中不可约．

337

证明 设 $\tilde{\varphi}:R[x]\to R/(p)[x]$ 是用 mod$p$ 约化系数的环同态，并设 $\tilde{f}(x)$ 表示 $\tilde{\varphi}(f(x))$．如果 $f(x)$ 在 $\mathrm{Frac}(R)[x]$ 中不是不可约的，则高斯定理，即系 6.27 给出多项式 $g(x),h(x)\in R[x]$ 使得 $f(x)=g(x)h(x)$，其中 $g(x)=b_0+b_1x+\cdots+b_mx^m$ 和 $h(x)=c_0+c_1x+\cdots+c_kx^k$．于是在 $R/(p)[x]$ 中有等式 $\tilde{f}(x)=\tilde{g}(x)\tilde{h}(x)$．

因 p 不能整除 a_n，所以有 $\tilde{f}(x)\neq 0$，事实上有某个单位 $u\in R/(p)$ 使得 $\tilde{f}(x)=ux^n$，这是因为除了 $\tilde{f}(x)$ 的首项系数外，其他一切系数都是 0. 根据定理 3.42，$R/(p)[x]$ 中的唯一因子分解，必有 $\tilde{g}(x)=vx^m$，其中 v 是 $R/(p)$ 中的单位，这是因为 $\tilde{g}(x)$ 的任一不可约因式也是 $\tilde{f}(x)$ 的不可约因式．同样，$\tilde{h}(x)=wx^k$，其中 w 是 $R/(p)$ 中的单位．由此，$\tilde{g}(x)$ 和 $\tilde{h}(x)$ 的常数项都是 0；即在 $R/(p)$ 中 $[b_0]=0=[c_0]$，等价地，$p\mid b_0$ 和 $p\mid c_0$. 但 $a_0=b_0c_0$，从而 $p^2\mid a_0$，产生矛盾．所以 $f(x)$ 在 $\mathrm{Frac}(R)[x]$ 中不可约． ■

当然，艾森斯坦准则对 $\mathbb{Z}[x]$ 中的多项式成立，可立即从 $\mathbb{Z}$ 推广到 PID.

系 6.35（高斯） 对每个素数 p，p 阶分圆多项式 $\Phi_p(x)$ 在 $\mathbb{Q}[x]$ 中不可约．

证明 因 $\Phi_p(x)=(x^p-1)/(x-1)$，所以有

$$\begin{aligned}\Phi_p(x+1)&=[(x+1)^p-1]/x\\&=x^{p-1}+\binom{p}{1}x^{p-2}+\binom{p}{2}x^{p-3}+\cdots+p.\end{aligned}$$

因 p 是素数，命题 1.12 表明艾森斯坦准则适用，由此可知 $\Phi_p(x+1)$ 在 $\mathbb{Q}[x]$ 中不可约．根据引理 6.33，$\Phi_p(x)$ 在 $\mathbb{Q}[x]$ 中不可约． ■

我们没有说当 n 不是素数时，$x^{n-1}+x^{n-2}+\cdots+x+1$ 是不可约的，例如 $x^3+x^2+x+1=(x+1)(x^2+1)$．

多元多项式的不可约性比一元多项式的不可约性更难判定，但这里有一个判别法．

命题 6.36 设 k 是域，并设 $f(x_1,\cdots,x_n)$ 是 $R[x_n]$ 中的本原多项式，其中 $R=k[x_1,\cdots,x_{n-1}]$．如果 f 不能因式分解为 $R[x_n]$ 中的两个较低次数的多项式，则 f 在 $k[x_1,\cdots,x_n]$ 中不可约．

证明 如果想把 f 看作 $R[x_n]$ 中的多项式，我们记 $f(x_1,\cdots,x_n)=F(x_n)$（当然，F 的系数是

$k[x_1,\cdots,x_{n-1}]$ 中的多项式）．假定 $F(x_n)=G(x_n)H(x_n)$，根据假设，G 和 H 的次数（关于 x_n）不能够都小于 $\deg(F)$，从而它们中的一个（比如 G）次数为 0. 因为 F 是本原的，从而 G 是 $k[x_1,\cdots,x_{n-1}]$ 中的一个单位．所以 $f(x_1,\cdots,x_n)$ 在 $R[x_n]=k[x_1,\cdots,x_n]$ 中不可约． ■

338

当然，这个命题可以应用到任意一个变量 x_i 上，而不只是 x_n．

系 6.37 *如果 k 是域且 $g(x_1,\cdots,x_n)$，$h(x_1,\cdots,x_n)\in k[x_1,\cdots,x_n]$ 互素，则 $f(x_1,\cdots,x_n,y)=yg(x_1,\cdots,x_n)+h(x_1,\cdots,x_n)$ 在 $k[x_1,\cdots,x_n,y]$ 中不可约．*

证明 设 $R=k[x_1,\cdots,x_n]$. 注意 f 在 $R[y]$ 中是本原的，这是由于 $(g,h)=1$ 迫使 f 的系数 g，h 的任一因子都是单位．因 f 关于 y 是线性的，它不是 $R[y]$ 中两个次数较小的多项式的乘积，因此命题 6.36 证明了 f 在 $R[y]=k[x_1,\cdots,x_n,y]$ 中不可约． ■

例如 xy^2+z 是本原多项式，它关于 x 是线性的，所以它是 $k[x,y,z]$ 中的不可约多项式．

习题

6.17 设 R 是 UFD 且 $Q=\mathrm{Frac}(R)$ 是它的分式域．证明每个非零元素 $a/b\in Q$ 都有一个既约表达式；即 a 和 b 互素．

6.18 设 R 是 UFD.

（i）如果 a，b，$c\in R$ 且 a 和 b 互素，证明 $a\mid bc$ 蕴涵 $a\mid c$．

（ii）如果 $a,c_1,\cdots,c_n\in R$ 且对一切 i 有 $c_i\mid a$，证明 $c\mid a$，其中 $c=\mathrm{lcm}\{c_1,\cdots,c_n\}$．

6.19 如果 R 是整环，证明 $R[x_1,\cdots,x_n]$ 中的单位都是 R 中的单位．另一方面，证明 $2x+1$ 是 $\mathbb{I}_4[x]$ 中的单位．

6.20 证明一个 UFD R 是 PID 当且仅当每个非零素理想都是极大理想．

6.21 （i）证明 x 和 y 在 $k[x,y]$ 中互素，其中 k 是域．

（ii）证明在 $k[x,y]$ 中 1 不是 x 和 y 的线性组合．

6.22 （i）证明对一切 $n\geqslant 1$，$\mathbb{Z}[x_1,\cdots,x_n]$ 是 UFD.

（ii）如果 R 是域，证明无限元多项式的环 $R=k[x_1,x_2,\cdots,x_n,\cdots]$ 也是 UFD.

提示： 我们还没有给出 R 的正式定义（这个定义将在第 8 章中给出），但对于本习题可把 R 看作升链 $k[x_1]\subsetneq k[x_1,x_2]\subsetneq\cdots\subsetneq k[x_1,x_2,\cdots,x_n]\subsetneq\cdots$ 的并．

6.23 判定下列多项式在 $\mathbb{Q}[x]$ 中是否不可约．

（i）$f(x)=3x^2-7x-5$.

（ii）$f(x)=2x^3-x-6$.

（iii）$f(x)=8x^3-6x-1$.

（iv）$f(x)=x^3+6x^2+5x+25$.

（v）$f(x)=x^4+8x+12$.

提示： 在 $\mathbb{F}_5[x]$ 中，$f(x)=(x+1)g(x)$，其中 $g(x)$ 是不可约的．

（vi）$f(x)=x^5-4x+2$.

（vii）$f(x)=x^4+x^2+x+1$.

提示： 证明 $f(x)$ 在 $\mathbb{F}_3$ 中没有根，而因系数的限制，$f(x)$ 不可能分解成二次多项式的乘积．

（viii）$f(x)=x^4-10x^2+1$.

339

提示： 证明 $f(x)$ 没有有理根，而因系数的限制，$f(x)$ 不可能分解成二次多项式的乘积．

6.24 x^5+x+1 在 $\mathbb{F}_2[x]$ 中不可约吗？

提示： 用例3.35（i）．

6.25 设 $f(x)=(x^p-1)/(x-1)$，其中 p 是素数．用恒等式

$$f(x+1)=x^{p-1}+pq(x),$$

其中 $q(x)\in\mathbb{Z}[x]$ 的常数项为 1，证明对一切 $n\geqslant 0$，$x^{p^n(p-1)}+\cdots+x^{p^n}+1$ 在$\mathbb{Q}[x]$中不可约．

6.26 （i）如果 a 是一个无平方因数的整数，证明对每个 $n\geqslant 1$，x^n-a 在$\mathbb{Q}[x]$中不可约．由此推出在$\mathbb{Q}[x]$中对每个 $n\geqslant 1$ 存在 n 次不可约多项式．

提示：用艾森斯坦准则．

（ii）如果 a 是一个无平方因数的整数，证明对一切 $n\geqslant 2$，$\sqrt[n]{a}$都是无理数．

6.27 设 k 是域，并设 $f(x)=a_0+a_1x+\cdots+a_nx^n\in k[x]$ 有次数 n 和非零常数项 a_0．证明：如果 $f(x)$ 是不可约的，则 $a_n+a_{n-1}x+\cdots+a_0x^n$ 也是不可约的．

6.28 设 k 是域，并设 $f(x_1,\cdots,x_n)\in k[x_1,\cdots,x_n]$ 是 $R[x_n]$ 中的本原多项式，其中 $R=k[x_1,\cdots,x_{n-1}]$．如果 f 关于 x_n 是二次或三次多项式，证明 f 在 $k[x_1,\cdots,x_n]$ 中不可约当且仅当 f 在 $k(x_1,\cdots,x_{n-1})$ 中没有根．

6.29 设 R 是 UFD 且 $Q=\mathrm{Frac}(R)$．如果 $f(x)\in R[x]$，证明 $f(x)$ 在 $R[x]$ 中不可约当且仅当 $f(x)$ 是本原的且 $f(x)$ 在 $Q[x]$ 中不可约．

6.30 证明

$$f(x,y)=xy^3+x^2y^2-x^5y+x^2+1$$

是$\mathbb{R}[x,y]$中的一个不可约多项式．

6.31 设 $D=\det\left(\begin{bmatrix}x & y\\ z & w\end{bmatrix}\right)$，从而 D 在多项式环$\mathbb{Z}[x,y,z,w]$中．

（i）证明 (D) 是$\mathbb{Z}[x,y,z,w]$中的素理想．

提示：证明 D 是一个不可约元素．

（ii）证明$\mathbb{Z}[x,y,z,w]/(D)$ 不是 UFD. 例 6.21 中给出另一个整环不是 UFD 的例子．

6.3 诺特环

当 k 是域时，$k[x_1,\cdots,x_n]$ 的最重要的性质之一是它的每个理想都可以由有限个元素生成．这个性质和理想的链密切相关，在证明 PID 是 UFD 的课题中我们已经看到过它．

定义 称交换环 R 满足 ACC，即**升链条件**，如果理想的每个升链

$$I_1\subseteq I_2\subseteq\cdots\subseteq I_n\subseteq\cdots$$

都有终止；即从某点开始序列变成常量：存在整数 N 使得 $I_N=I_{N+1}=I_{N+2}=\cdots$. [340]

引理6.18（ii）表明每个 PID 满足 ACC.

下面是理想的一个重要类型．

定义 如果 X 是交换环 R 的子集，则由 X **生成的理想**是指一切有限线性组合的集合

$$I=(X)=\Big\{\sum_{\text{有限}}r_ia_i:r_i\in R\text{ 且 }a_i\in X\Big\}.$$

如果 $X=\{a_1,\cdots,a_n\}$，我们说 I 是**有限生成的**，常缩写为 f. g.；即 I 中的每个元素都是 a_i 的 R-线性组合．记

$$I=(a_1,\cdots,a_n),$$

并称 I 为 a_1，…，a_n **生成的理想**．

理想 I 的生成元 a_1，…，a_n 的集合有时叫做 I 的**基**（尽管和向量空间的基相比这是一个较弱的概念，这里我们没有假定表达式 $c=\sum r_ia_i$ 中的系数 r_i 被 c 唯一确定）．

当然，PID 中的每个理想都是有限生成的，因为它能够由一个元素生成．

命题6.38 对交换环 R，下列条件等价．

（i） R 有 ACC.

（ii） R 满足**极大条件**：R 中理想的每个非空族 $\mathcal{F}$ 有极大元素，即存在 $I_0 \in \mathcal{F}$，对于它没有 $I \in \mathcal{F}$ 能够满足 $I_0 \subsetneq I$.

（iii） R 中的每个理想都是有限生成的．

证明 （i）⇒（ii）：设 $\mathcal{F}$ 是 R 中理想的族，并假定 $\mathcal{F}$ 中没有极大元素．选取 $I_1 \in \mathcal{F}$，因 I_1 不是极大元素，存在 $I_2 \in \mathcal{F}$ 使得 $I_1 \subsetneq I_2$. 现在 I_2 不是 $\mathcal{F}$ 中的极大元素，从而存在 $I_3 \in \mathcal{F}$ 使得 $I_2 \subsetneq I_3$. 如此继续，我们可以构造出一个没有终止的 R 中理想的升链，与 ACC 矛盾．

（ii）⇒（iii）：设 I 是 R 的理想，并定义 $\mathcal{F}$ 为包含在 I 中的一切有限生成的理想族．当然，$\mathcal{F} \neq \varnothing$（因为 $\{0\} \in \mathcal{F}$）．根据假设，存在极大元素 $M \in \mathcal{F}$．现在因为 $M \in \mathcal{F}$，所以 $M \subseteq I$. 如果 $M \subsetneq I$，则存在 $a \in I$ 而 $a \notin M$. 理想

$$J = \{m + ra : m \in M \text{和} r \in R\} \subseteq I$$

是有限生成的，因此 $J \in \mathcal{F}$，而 $M \subsetneq J$，这便和 M 的极大性矛盾．所以 $M = I$，I 是有限生成的．

（iii）⇒（i）：假定 R 中的每个理想都是有限生成的，并设

341

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

是 R 中理想的升链．根据引理6.18（i），该升链的并 $J = \bigcup_{n \geqslant 1} I_n$ 是理想．

由假设，存在元素 $a_i \in J$ 使得 $J = (a_1, \cdots, a_q)$．现在 a_i 取自 J，必有某个 n_i 使得 $a_i \in I_{n_i}$．如果 N 是 n_i 中最大的一个，则对一切 i，$I_{n_i} \subseteq I_N$，因此对一切 i，$a_i \in I_N$，从而

$$J = (a_1, \cdots, a_q) \subseteq I_N \subseteq J.$$

由此，如果 $n \geqslant N$，则 $J = I_N \subseteq I_n \subseteq J$，因此 $I_n = J$. 所以链终止，R 有 ACC. ■

我们现在对满足命题中三个等价条件中任意一个的交换环给予一个名称．

定义 如果交换环 R 中的每个理想都是有限生成的，则称交换环 R 为**诺特环**㊀.

我们马上会看到当 k 是域时，$k[x_1, \cdots, x_n]$ 是诺特环．另一方面，下面是非诺特交换环的一个例子．

例6.39 设 $R = \mathcal{F}(\mathbb{R})$ 是实数域上一切实值函数的环，其运算为点态运算（见例3.7）．易知，对每个正整数 n，

$$I_n = \{f : \mathbb{R} \to \mathbb{R} : f(x) = 0, \text{对一切 } x \geqslant n\}$$

是理想，并对一切 n 有 $I_n \subsetneq I_{n+1}$. 所以 R 不满足 ACC，从而 R 不是诺特环． ■

下面是极大条件的应用．

系6.40 如果 I 是诺特环 R 中的真理想，则存在 R 中包含 I 的极大理想 M. 特别地，每个诺特环都有极大理想．㊁

证明 设 $\mathcal{F}$ 是 R 中包含 I 的一切真理想的族．注意，因为 $I \in \mathcal{F}$，所以 $\mathcal{F} \neq \varnothing$. 因 R 是诺特环，极大条件给出 $\mathcal{F}$ 中的极大元素 M. 我们还需证明 M 是 R 中的极大理想（即 M 是 R 中一切真理想组成的更大族 $\mathcal{F}'$ 中的极大元素）．假定存在真理想 J 满足 $M \subseteq J$，则 $I \subseteq J$，从而 $J \in \mathcal{F}$，因而由 M 的极大性得 $M = J$，所以 M 是 R 中的极大理想． ■

㊀ 这个名称是为纪念诺特（Emmy Noether，1882—1935），她于1921年引入链条件．

㊁ 这个系没有 R 是诺特环的假设也成立，但一般结果的证明要用到佐恩引理；见定理6.46.

下面是从一个老的诺特环构造新诺特环的一种方法．

342

系 6.41 如果 R 是诺特环且 I 是 R 中的理想，则 R/I 也是诺特环．

证明 如果 A 是 R/I 中的理想，则对应定理给出 R 中的理想 J 满足 $J/I=A$. 因 R 是诺特环，所以理想 J 是有限生成的，比如 $J=(b_1,\cdots,b_n)$，从而 $A=J/I$ 也是有限生成的（由陪集 $b_1+I,\cdots,b_n+I$ 生成）．所以 R/I 是诺特环． ■

下面的轶闻众所周知．大约在 1890 年，希尔伯特证明了著名的希尔伯特基定理，该定理表明 $\mathbb{C}[x_1,\cdots,x_n]$ 中的每个理想都是有限生成的．我们会看到这个证明没有给出一个理想的明确的生成元，在此意义下它是非构造性的．传说戈丹（P. Gordan）（当时的领衔代数学家之一）第一次看到希尔伯特的证明时说，“这不是数学，而是神学！”另一方面，当 1899 年戈丹发表希尔伯特定理的一个简化证明时说，“我使自己信服神学也有它的好处．”

下面给出的希尔伯特基定理的证明属于 H. Sarges (1976)．

定理 6.42（希尔伯特基定理） 如果 R 是交换诺特环，则 $R[x]$ 也是诺特环．

证明 假定 I 是 $R[x]$ 中的理想，它不是有限生成的，当然 $I\neq\{0\}$．定义 $f_0(x)$ 为 I 中具有极小次数的多项式，并归纳定义 $f_{n+1}(x)$ 为 $I-(f_0,\cdots,f_n)$ 中具有极小次数的多项式．注意，$f_n(x)$ 对所有 $n\geqslant 0$ 存在；如果 $I-(f_0,\cdots,f_n)$ 是空的，则 I 就是有限生成的．显然

$$\deg(f_0)\leqslant\deg(f_1)\leqslant\deg(f_2)\leqslant\cdots.$$

令 a_n 表示 $f_n(x)$ 的首项系数．因 R 是诺特环，应用习题 6.32 给出整数 m 使得 $a_{m+1}\in(a_0,\cdots,a_m)$，即存在 $r_i\in R$ 使得 $a_{m+1}=r_0a_0+\cdots+r_ma_m$. 定义

$$f^*(x)=f_{m+1}(x)-\sum_{i=0}^{m}x^{d_{m+1}-d_i}r_if_i(x),$$

其中 $d_i=\deg(f_i)$．现在 $f^*(x)\in I-(f_0(x),\cdots,f_m(x))$，否则 $f_{m+1}(x)\in(f_0(x),\cdots,f_m(x))$. 只要证明 $\deg(f^*)<\deg(f_{m+1})$，这是因为这和 $f_{m+1}(x)$ 在属于 I 而不属于 $(f_0,\cdots,f_m)$ 的多项式中具有极小次数矛盾．如果 $f_i(x)=a_ix^{d_i}+$ 低次项，则

$$\begin{aligned}f^*(x)&=f_{m+1}(x)-\sum_{i=0}^{m}x^{d_{m+1}-d_i}r_if_i(x)\\&=(a_{m+1}x^{d_{m+1}}+\text{低次项})-\sum_{i=0}^{m}x^{d_{m+1}-d_i}r_i(a_ix^{d_i}+\text{低次项}).\end{aligned}$$

于是，被减去的首项是 $\sum_{i=0}^{m}r_ia_ix^{d_{m+1}}=a_{m+1}x^{d_{m+1}}$. ■

343

系 6.43 (i) 如果 k 是域，则 $k[x_1,\cdots,x_n]$ 是诺特环．

(ii) 环 $\mathbb{Z}[x_1,\cdots,x_n]$ 是诺特环．

(iii) 对 $k[x_1,\cdots,x_n]$ 中的每个理想 I，商环 $k[x_1,\cdots,x_n]/I$ 是诺特环，其中 $k=\mathbb{Z}$ 或 k 是域．

证明 (i)，(ii) 用定理对 $n\geqslant 1$ 作归纳证明．(iii) 的证明从系 6.41 可得． ■

习题

6.32 设 R 是交换环．证明 R 是诺特环，当且仅当对 R 中元素的任一序列 $a_1, a_2, \cdots, a_n, \cdots$，存在整数 $m\geqslant 1$ 使得 a_{m+1} 是它前面元素的 R-线性组合；即存在 $r_1, \cdots, r_m\in R$ 使得 $a_{m+1}=r_1a_1+\cdots+r_ma_m$.

6.33 (i) 举出一个诺特环 R 的例子，它包含一个非诺特的子环．

(ii) 举出一个交换环 R 的例子，它包含真理想 $I\subsetneq J\subsetneq R$ 满足 J 是有限生成的，而 I 不是有限生成的．

6.34 设 R 是诺特整环使得每个 a，$b\in R$ 有 gcd，而且这个 gcd 是 a 和 b 的 R-线性组合．证明 R 是 PID.（诺特环的假设是必要的，因为存在非诺特整环，叫做贝祖（Bézout）环，其中每个有限生成的理想都是主理想．）

提示：对一个理想的生成元的个数用归纳法．

6.35 不用命题 6.38 证明 PID R 中理想的每个非空族$\mathcal{F}$有极大元素．

6.36 例 6.39 证明了 $R=\mathcal{F}(\mathbb{R})$，即$\mathbb{R}$上的一切函数在点态运算下的环不满足 ACC.

（i）证明在例 6.39 中理想的族 $\{I_n : n\geqslant 1\}$ 没有极大元素．

（ii）定义

$$f_n(x)=\begin{cases}1 & \text{如果 } x<n\\ 0 & \text{如果 } x\geqslant n,\end{cases}$$

并定义 $J_n=(f_1,\cdots,f_n)$．证明 $J^*=\bigcup_{n\geqslant 1} J_n$ 是理想但不是有限生成的．

6.37 如果 R 是交换环，归纳定义多元形式幂级数的环为

$$R[[x_1,\cdots,x_{n+1}]]=A[[x_{n+1}]],$$

其中 $A=R[[x_1,\cdots,x_n]]$．

证明：如果 R 是诺特环，则 $R[[x_1,\cdots,x_n]]$ 也是诺特环．

提示：如果 $n=1$，则用习题3.54(i)．当 $n\geqslant 1$ 时，用希尔伯特基定理的证明，但用幂级数的阶替换多项式的次数（一个非零幂级数$\sum c_i x^i$ 的阶是满足 $c_i\neq 0$ 的最小 i）．

344

6.38 设

$$S^2=\{(a,b,c)\in\mathbb{R}^3 : a^2+b^2+c^2=1\}$$

是$\mathbb{R}^3$ 中的单位球面，并设

$$I=\{f(x,y,z)\in\mathbb{R}[x,y,z] : \text{对一切}(a,b,c)\in S^2, f(a,b,c)=0\}.$$

证明 I 是$\mathbb{R}[x,y,z]$ 中有限生成的理想．

6.39 如果 R 和 S 都是诺特环，证明它们的直积 $R\times S$ 也是诺特环．

6.40 如果 R 是交换环，而且它也是域 k 上的向量空间，则称 R 为**交换 k-代数**，如果对一切 $\alpha\in k$ 和 u，$v\in R$ 有

$$(\alpha u)v=\alpha(uv)=u(\alpha v).$$

证明 k 上每个有限维交换 k-代数都是诺特环．

6.4 佐恩引理的应用

处理无限集合需要一些集合论的适当的工具．

定义 如果 A 是集合，记它的一切非空子集的族为$\mathcal{P}(A)^\#$．**选择公理**声称，如果 A 是非空集合，则存在函数 $\beta:\mathcal{P}(A)^\#\to A$ 使得对 A 的每个非空子集 S，$\beta(S)\in S$．这样的函数 β 叫做**选择函数**.

非正式地说，选择公理看起来是一个无关紧要的陈述，它说我们可以从一个集合的每个子集中同时选取一个元素．

选择公理是容易接受的，而且它是集合论的标准公理之一．事实上，选择公理和非空集合的笛卡儿积非空的说法是等价的（见附录，命题 A.1）．然而，公理的原来形式用起来是不方便的．存在各种更有用的等价形式，最流行的是*佐恩引理*和*良序原则*.

回忆如果在集合 X 上定义了一个自反的、反对称的、传递的关系 $x\preceq y$，则称 X 为*偏序集*.

下面介绍几个定义使我们能够陈述良序原则．

定义 偏序集 X 称为**良序的**，如果 X 的每个非空子集 S 包含**最小元素**，即存在 $s_0 \in S$ 使得

$$对一切\ s \in S, s_0 \leq s.$$

自然数$\mathbb{N}$的集合是良序的（这正是第1章中最小整数公理所陈述的），但一切整数的集合$\mathbb{Z}$不是良序的，因为$\mathbb{Z}$自身是子集，它没有最小元素．

良序原则 每个集合 X 都有它的元素的某个良序．

345

如果 X 是一个偏序集，则由良序原则，必存在一个良序，这个良序可能不是原来的偏序也可能就是原来的偏序．例如$\mathbb{Z}$可以排成良序：

$$0 \preceq 1 \preceq -1 \preceq 2 \preceq -2 \preceq \cdots.$$

在下面的定义之后，我们可以陈述佐恩引理．

定义 偏序集 X 中的元素 m 称为**极大元素**，如果不存在 $x \in X$ 满足 $m \prec x$；即

$$如果\ m \preceq x, 则\ m = x.$$

回忆偏序集 X 的非空子集 Y 的上界是指元素 $x_0 \in X$ 满足对每个 $y \in Y$ 有 $y \preceq x_0$，但并不要求这个 x_0 在 Y 中．

例 6.44 （ⅰ）一个偏序集可以没有极大元素．例如$\mathbb{R}$在常序下没有极大元素．

（ⅱ）一个偏序集可以有许多极大元素．例如 X 是集合 U 的一切真子集组成的偏序集，则子集 S 是极大元当且仅当 $S = U - \{u\}$，其中 $u \in U$，即 S 是一点的补集．

（ⅲ）如果 X 是交换环 R 中的一切真理想的族，偏序为包含，则 X 中的极大元素就是极大理想． ■

佐恩引理给出了一个保证极大元素存在的条件．

定义 称偏序集 X 为**链**，如果对一切 x，$y \in X$，不是 $x \preceq y$ 就是 $y \preceq x$.

实数$\mathbb{R}$的集合是链，如果取 $x \preceq y$ 为通常的不等性 $x \leqslant y$.

佐恩引理 如果 X 是非空偏序集，其中的每个链在 X 中都有上界，则 X 有极大元素．

定理 下列陈述等价：

（ⅰ）佐恩引理．

（ⅱ）良序原则．

（ⅲ）选择公理．

证明 见附录． ■

今后我们将毫无顾忌地假定所有这些陈述都是真的，并在需要的时候使用它们．

下一命题经常用来验证佐恩引理的假设成立．

346

命题 6.45 如果 C 是链且 $S = \{x_1, \cdots, x_n\} \subseteq C$，则存在某个 x_i，其中 $1 \leqslant i \leqslant n$，使得对一切 $x_j \in S$ 有 $x_j \preceq x_i$.

证明 对 $n \geqslant 1$ 用归纳法证明．基础步显然为真．设 $S = \{x_1, \cdots, x_{n+1}\}$，并定义 $S' = \{x_1, \cdots, x_n\}$. 归纳假设给出 x_i，其中 $1 \leqslant i \leqslant n$，使得对一切 $x_j \in S'$ 有 $x_j \preceq x_i$. 因 C 是链，所以 $x_i \preceq x_{n+1}$ 或 $x_{n+1} \preceq x_i$. 两种情形都给出了 S 的极大元素． ■

下面是佐恩引理的第一个应用．

定理 6.46 如果 R 是非零交换环，则 R 有极大理想．事实上，R 中的每个真理想 I 都包含在一个极大理想中．

证明 第二个陈述蕴涵了第一个，因为 R 是非零环，所以理想$\{0\}$是真理想，从而存在 R 中的极大理想包含它．

设 X 是包含 I 的一切真理想的族（注意，因为 $I\in X$，所以 $X\neq\varnothing$），用包含作为 X 的偏序．易知 X 的极大元素是 R 中的极大理想：不存在真理想严格包含它．

设$\mathcal{C}$是 X 的一个链，于是给定 I，$J\in\mathcal{C}$，$I\subseteq J$ 或 $J\subseteq I$. 我们断言 $I^*=\bigcup_{I\in\mathcal{C}} I$ 是$\mathcal{C}$的一个上界．显然对一切 $I\in\mathcal{C}$，$I\subseteq I^*$，所以剩下的只要证明 I^* 是真理想．I^* 是理想的论证现在已经熟悉．最后我们证明 I^* 是真理想．如果 $I^*=R$，则 $1\in I^*$. 1 取自 I^* 必有某个 $I\in\mathcal{C}$使得 $1\in I$，这与 I 是真理想矛盾．

我们已经验证了 X 的每个链有上界，因此佐恩引理给出所要的极大元素． ■

注 如果环 R 的定义中不强调 R 必需包含 1，则定理 6.46 不成立．这种“没有单位的环”的例子是任一加法阿贝尔群 G，在其上定义乘法为对一切 a，$b\in G$，$ab=0$. 理想的通常定义有意义，且易知 G 中的理想是它的子群．于是一个极大理想 I 恰是一个极大子群，由对应定理，这意味着 G/I 没有真子群．于是 G/I 是阿贝尔单群，即 G/I 是素数阶有限群．特别地，取 $G=\mathbb{Q}$ 作为加法阿贝尔群，并配置零乘法．读者可以证明$\mathbb{Q}$没有非零的有限商群，因此它没有极大子群．所以这个“没有单位的环”没有极大理想．

对一个偏序集 X 运用佐恩引理时，我们强调必需验证 X 非空．例如，一个粗心人会断言佐恩引理可用来证明存在$\mathbb{Z}$的极大不可数子集．定义 X 为$\mathbb{Z}$的一切不可数子集的集合，并用包含作为 X 的偏序．如果 C 是 X 中的链，则显然不可数子集 $S^*=\bigcup_{S\in C} S$ 是 C 的一个上界，这是因为对每个 $S\in C$ 有 $S\subseteq S^*$. 所以佐恩引理给出 X 的极大元素，它必是$\mathbb{Z}$的极大不可数子集．当然，其破绽是 $X=\varnothing$（因为可数集的每个子集也是可数集）．

347

下面是佐恩引理的第二个应用．我们先把向量空间的基的通常定义加以推广，使它适用于一切向量空间，而不必限于有限维的．

定义 设 V 是某个域 k 上的向量空间，并设 $Y\subseteq V$ 是一个无限子集．㊀

（ⅰ）称 Y **线性无关**，如果 Y 的每个有限子集线性无关．

（ⅱ）称 Y 张成 V，如果每个 $v\in V$ 是 Y 中有限㊁个元素的线性组合．当 V 由 Y 张成时，记为 $V=\langle Y\rangle$.

（ⅲ）向量空间 V 的一个**基**是指一个张成 V 的线性无关的子集．

由此，一个无限子集 $Y=\{y_i: i\in I\}$线性无关，如果一旦 $\sum a_i y_i=0$（其中只有有限个 $a_i\neq 0$），则对一切 i 有 $a_i=0$.

例 6.47 设 k 是域，并把 $V=k[x]$看作 k 上的向量空间．我们断言

$$Y=\{1,x,x^2,\cdots,x^n,\cdots\}$$

是 V 的基．因为任意一个 d 次多项式是 1，x，x^2，…，x^d 的 k -线性组合，所以 Y 张成 V. 因为不存在不全为 0 的标量 a_0，a_1，…，a_n 满足 $\sum_{i=0}^{n} a_i x^i=0$（一个多项式只有在所有系数都为 0 时才是零多项式），所以 Y 也线性无关．因此 Y 是 V 的基． ■

㊀ 涉及无限基的时候，用子集替代表较方便．

㊁ 只有 V 中元素的有限和是允许的．没有极限，无穷级数的收敛性便没有意义，因此无限个非零项的和没有定义．

定理 6.48 域 F 上的每个向量空间 V 都有基．事实上，V 的任一线性无关的子集 B 都包含在 V 的一个基之中；即存在子集 B' 使得 $B\cup B'$ 是 V 的基．

证明 注意第一个陈述可由第二个得出，因为 $B=\varnothing$ 是一个线性无关的子集，它包含在一个基之中．

设 X 是 V 的一切包含 B 的线性无关的子集族．因为 $B\in X$，所以族 X 非空．用包含作为 X 的偏序．我们用佐恩引理证明 X 中存在极大元素．设 $\mathcal{B}=\{B_j: j\in J\}$ 是 X 的链．于是每个 B_j 都是包含 B 的线性无关的子集，且对一切 i，$j\in J$，$B_i\subseteq B_j$ 或 $B_j\subseteq B_i$．如果 $B_{j_1},\cdots,B_{j_n}$ 是这些 B_j 的任一有限族，则由命题 6.45，其中一个包含所有其他各个子集．

令 $B^*=\bigcup_{j\in J}B_j$．显然 B^* 包含 B，且对一切 $j\in J$，$B_j\subseteq B^*$．由此，如果 B^* 属于 X，即如果 B^* 是 V 的线性无关子集，则 B^* 就是 $\mathcal{B}$ 的一个上界．如果 B^* 不是线性无关的，则它有线性相关的有限子集 $y_{i_1},\cdots,y_{i_m}$．y_{i_k} 怎么放进 B^* 的？答案是有某个指标 j_k 满足 $y_{i_k}\in B_{j_k}$．因只有有限个 y_{i_k}，所以存在 B_{j_0} 包含一切 B_{j_k}，即 $y_{i_1},\cdots,y_{i_m}\in B_{j_0}$．但根据假设，$B_{j_0}$ 是线性无关的，这是一个矛盾．所以 B^* 是全序子集 $\mathcal{B}$ 的一个上界．我们已经验证了 X 的每个链有上界，因此运用佐恩引理可知 X 中存在极大元素．

348

设 M 是 X 中的极大元素．因 M 线性无关，只要证明它张成 V（因为只要 M 张成 V，它就是 V 的包含 B 的基）．如果 M 不能张成 V，则存在 $v_0\in V$ 满足 $v_0\notin(M)$，(M) 是由 M 张成的子空间．考虑子集 $M^*=M\cup\{v_0\}$．显然 $M\subsetneq M^*$．现在 M^* 是线性无关的：如果 $a_0v_0+\sum a_iy_i=0$，其中 $y_i\in M$，且 a_0，$a_i\in F$ 不全为 0，则 $a_0\neq 0$（否则出现在等式中的那些 y_i 的集合将是线性相关的，产生矛盾）．但如果 $a_0\neq 0$，则 $v_0=-a_0^{-1}\sum a_iy_i$，与 $v_0\notin(M)$ 矛盾．所以 M 是 V 的基．最后的陈述只要定义 $B'=M-B$ 即可． ■

回忆一个向量空间 V 的子空间 W 称为一个**直和项**，如果存在 V 的子空间 W' 满足 $\{0\}=W\cap W'$ 且 $V=W+W'$（即每个 $v\in V$ 可以写成 $v=w+w'$，其中 $w\in W$ 和 $w'\in W'$）．我们说 V 是 W 和 W' 的**直和**，并记为 $V=W\oplus W'$．

系 6.49 向量空间 V 的每个子空间 W 都是一个直和项．

证明 设 B 是 W 的基．根据定理，存在子集 B' 使得 $B\cup B'$ 是 V 的基．容易验证 $V=W\oplus\langle B'\rangle$，其中 $\langle B'\rangle$ 表示 B' 张成的子空间． ■

实数 $\mathbb{R}$ 的环是 $\mathbb{Q}$ 上的向量空间，常称它的一个基为**哈梅尔(Hamel)基**，它在构造分析反例中有用．例如我们可以用哈梅尔基证明存在满足函数方程 $f(x+y)=f(x)+f(y)$ 的不连续函数 $f:\mathbb{R}\to\mathbb{R}$.[⊖]

例 6.50 域 k 上向量空间 V 上的内积是指函数

⊖ 这里是用无限基数概要证明存在这种不连续函数 f. 和有限维情形一样，如果 B 是向量空间 V 的基，则任一函数 $f:B\to V$ 可以扩张为一个线性变换 $F:V\to V$（见命题 7.49），它就是 $F(\sum r_ib_i)=\sum r_if(b_i)$．一个哈梅尔基有基数 $c=|\mathbb{R}|$，从而有 $c^c=2^c>c$ 个函数 $f:\mathbb{R}\to\mathbb{R}$ 满足这个函数方程，这是因为每个线性变换都是可加的．另一方面，$\mathbb{R}$ 上的每个连续函数由它在 $\mathbb{Q}$ 上的值所确定，$\mathbb{Q}$ 是可数的，从而 $\mathbb{R}$ 上只有 c 个连续函数．所以存在不连续函数 $f:\mathbb{R}\to\mathbb{R}$ 满足函数方程 $f(x+y)=f(x)+f(y)$．

我们已经证明了存在一个不连续函数 $f:\mathbb{R}\to\mathbb{R}$ 对一切 $x,y\in\mathbb{R}$ 有 $f(x+y)=f(x)+f(y)$，即存在某个 $a\in\mathbb{R}$ 使得 f 在 a 处不连续．于是存在某个 $\epsilon>0$ 使得对每个 $\delta>0$ 有一个 $b\in\mathbb{R}$ 满足 $|b-a|<\delta$ 且 $|f(b)-f(a)|\geqslant\epsilon$．我们证明 f 在每个 $c\in\mathbb{R}$ 处不连续．恒等式 $b-a=(b+c-a)-c$ 给出 $|(b+c-a)-c|<\delta$，恒等式 $f(b+c-a)-f(c)=f(b)-f(a)$ 又给出 $|f(b+c-a)-f(c)|\geqslant\epsilon$．

$$V \times V \to k,$$

它的值记为 (v,w)，满足

349

（i）对一切 $v,v',w \in V$，$(v+v',w) = (v,w)+(v',w)$；

（ii）对一切 v，$w\in V$ 和 $\alpha \in k$，$(\alpha v,w) = \alpha(v,w)$；

（iii）对一切 $v,w \in V$，$(v,w) = (w,v)$.

如果当 $v\neq 0$ 时有 $(v,v) \neq 0$，我们就说这个内积是**确定的**.

我们要用哈梅尔基给出$\mathbb{R}$上的一个确定的内积，它的一切值都是有理数．把$\mathbb{R}$看作$\mathbb{Q}$上的向量空间，并设 Y 是基．对每个 u，$v\in \mathbb{R}$，存在 $y_i\in Y$ 和有理数 a_i，b_i 使得 $v=\sum a_i y_i$ 和 $w=\sum b_i y_i$，必要时可用 0 系数（非零的 a_i 和非零的 b_i 分别由 v 和 w 唯一确定）．定义

$$(v,w) = \sum a_i b_i;$$

注意这个和只有有限个非零项．容易验证我们定义了一个确定的内积． ■

无限维向量空间有维数的概念，当然现在的维数是基数．在下面的证明中，将引用几个基数的事实．我们将一个集合 X 的基数记为 $|X|$.

事实Ⅰ *设 X 和 Y 都是集合，并设 $f: X\to Y$ 是函数. 如果对每个 $y\in Y$，$f^{-1}(y)$是有限的，则 $|X| \leqslant \aleph_0 |Y|$．因此，如果 Y 是无限的，则 $|X| \leqslant |Y|$.*

见 Kaplansky 所著的《Set Theory and Metric Spaces》；因 X 是不相交并 $X=\bigcup_{y\in Y} f^{-1}(y)$，所以该结果可由该书 43 页定理 16 得到．

事实Ⅱ *如果 X 是一个无限集，$\mathrm{Fin}(X)$ 是它的一切有限子集的族，则 $|\mathrm{Fin}(X)| = |X|$.*

见 Kaplansky 所著的《Set Theory and Metric Spaces》；这个结果也由定理 16 得到．

事实Ⅲ（施罗德-伯恩斯坦定理） *如果 X 和 Y 都是集合，且满足 $|X| \leqslant |Y|$ 和 $|Y| \leqslant |X|$，则 $|X| = |Y|$.*

见 Birkhoff-Mac Lane 所著的《A Survey of Modern Algebra》387 页．

定理 6.51 *设 k 是域且 V 是 k 上的向量空间．*

*（i）V 的任意两个基有相同的元素个数（即它们有相同的基数）. 这个基数叫做 V 的**维数**并记为 $\dim(V)$.*

（ii）域 k 上的向量空间 V 和 V' 同构当且仅当 $\dim(V) = \dim(V')$.

证明 （i）设 B 和 B' 都是 V 的基．如果 B 有限，则 V 是有限维的，因此 B' 也是有限的（系 3.90）．此外在定理 3.85 中我们已经证明 $|B| = |B'|$．所以可以假定 B 和 B' 都是无限的．

每个 $v\in V$ 有唯一的形如 $v = \sum_{b\in B} \alpha_b b$ 的表达式，其中 $\alpha_b\in k$ 且几乎一切 $\alpha_b=0$. 定义 v 的**支撑**(关于 B 的）为

350

$$\mathrm{supp}(v) = \{b \in B : \alpha_b \neq 0\};$$

于是对每个 $v \in V$，$\mathrm{supp}(v)$ 是 B 的有限子集．定义 $f: B'\to \mathrm{Fin}(B)$ 为 $f(b') = \mathrm{supp}(b')$．注意，如果 $\mathrm{supp}(b') = \{b_1,\cdots,b_n\}$，则 $b' \in \langle b_1,\cdots,b_n\rangle = \langle \mathrm{supp}(b')\rangle$，它是由 $\mathrm{supp}(b')$ 张成的子空间. 因 $\langle \mathrm{supp}(b')\rangle$ 的维数是 n，而 B' 是无关的，所以 $\langle \mathrm{supp}(b')\rangle$ 最多包含 B' 的 n 个元素（系 3.88）．因此对 B 的每个有限子集 T，$f^{-1}(T)$ 是有限的［当然，有可能 $f^{-1}(T) = \varnothing$］．根据事实Ⅰ，有 $|B'| \leqslant |\mathrm{Fin}(B)|$，再根据事实Ⅱ，有 $|B'| \leqslant |B|$．交换 B 和 B' 的角色得相反的不等式 $|B| \leqslant |B'|$，从而事实Ⅲ给出 $|B'| = |B|$.

（ii）只要修改系 3.105 对有限维情形的证明即可． ■

下一个应用是用诺特环的素理想来刻画诺特环．

引理 6.52 设 R 是交换环，并设$\mathcal{F}$是 R 中一切非有限生成的理想的族．如果$\mathcal{F}\neq\varnothing$，则$\mathcal{F}$有极大元素．

证明 用包含作为$\mathcal{F}$的偏序．根据佐恩引理，只要证明：如果$\mathcal{C}$是$\mathcal{F}$中的链，则 $I^*=\bigcup_{I\in X} I$ 不是有限生成的．如果相反，$I^*=(a_1,\cdots,a_n)$，则有某个 $I_j\in\mathcal{C}$使得 $a_j\in I_j$．而$\mathcal{C}$是链，因此根据命题 6.45，理想 I_1，…，I_n 中有一个（比如叫它 I_0）包含其他各个．从而 $I^*=(a_1,\cdots,a_n)\subseteq I_0$．因为对所有的 $I\in\mathcal{C}$有 $I\subseteq I^*$，所以反包含 $I_0\subseteq I^*$ 是显然的．于是 $I_0=I^*$ 是有限生成的，与 $I_0\in\mathcal{F}$ 矛盾． ■

定理 6.53（科恩） 交换环 R 是诺特环当且仅当 R 中的每个素理想都是有限生成的．

证明 只需证明充分性．假定每个素理想都是有限生成的．令$\mathcal{F}$是 R 中一切非有限生成的理想的族．如果$\mathcal{F}\neq\varnothing$，则引理给出一个非有限生成的理想 I，它是非有限生成的理想中的极大的一个．我们要证明 I 是素理想，从而和假设每个素理想都是有限生成的矛盾，因此$\mathcal{F}=\varnothing$，即 R 是诺特环．

假设 $ab\in I$ 而 $a\notin I$ 且 $b\notin I$. 因 $a\notin I$，理想 $I+Ra$ 严格大于 I，从而 $I+Ra$ 是有限生成的．于是可以假定

$$I+Ra=(i_1+r_1a,\cdots,i_n+r_na),$$

其中对一切 $k,i_k\in I,r_k\in R$. 考虑 $J=(I:a)=\{x\in R:xa\in I\}$．现在 $I+Rb\subseteq J$；因 $b\notin I$，所以有 $I\subsetneq J$，从而 J 是有限生成的．我们断言 $I=(i_1,\cdots,i_n,Ja)$．因为每个 $i_k\in I$ 和 $Ja\subseteq I$，显然 $(i_1,\cdots,i_n,Ja)\subseteq I$．关于反包含，如果 $z\in I\subseteq I+Ra$，则有 $u_k\in R$ 使得 $z=\sum_k u_k(i_k+r_ka)$．于是 $(\sum_k u_kr_k)a=z-\sum_k u_ki_k\in I$，从而 $\sum_k u_kr_k\in J$，因此 $z=\sum_k u_ki_k+(\sum_k u_kr_k)a\in(i_1,\cdots,i_n,Ja)$. 由此，$I=(i_1,\cdots,i_n,Ja)$ 是有限生成的，产生矛盾，因此 I 是素理想． ■

克鲁尔（W. Krull）证明每个诺特环有素理想上的 DCC（见系 11.163）. 351

下一个应用涉及域的代数闭包．回忆一个域扩张 K/k 是代数扩张，如果每个 $a\in K$ 都是某个非零多项式 $f(x)\in k[x]$ 的根；即 K/k 是代数扩张，如果每个元素 $a\in K$ 都是 k 上的代数元素．

我们已经在命题 3.117 中讨论过代数扩张，下面的命题再扩充一点．

命题 6.54 设 K/k 是一个扩张．

（i）如果 $z\in K$，则 z 是 k 上的代数元素当且仅当 $k(z)/k$ 是有限的．

（ii）如果 $z_1,z_2,\cdots,z_n\in K$ 是 k 上的代数元素，则 $k(z_1,z_2,\cdots,z_n)/k$ 是有限扩张．

（iii）如果 y，$z\in K$ 是 k 上的代数元素，则 $y+z$，yz 和 y^{-1}（对 $y\neq0$）也是 k 上的代数元素．

（iv）定义

$$K_{\text{alg}}=\{z\in K: z\text{ 是 }k\text{ 上的代数元素}\}.$$

则 K_{alg}是 K 的子域．

证明 （i）如果 $k(z)/k$ 是有限的，则命题3.117（i）表明 z 是 k 上的代数元素．反之，如果 z 是 k 上的代数元素，则命题3.117（v）表明 $k(z)/k$ 是有限的．

（ii）对 $n\geqslant1$ 用归纳法证明．基础步是（i）．关于归纳步，存在域塔

$$k\subseteq k(z_1)\subseteq k(z_1,z_2)\subseteq\cdots\subseteq k(z_1,\cdots,z_n)\subseteq k(z_1,\cdots,z_{n+1}).$$

现在 $[k(z_{n+1}):k]$ 是有限的，并根据归纳假设，$[k(z_1,\cdots,z_n):k]$ 是有限的．事实上，$[k(z_{n+1}):k]=d$，其中 d 是 $k[x]$ 中以 z_{n+1} 为根的首一不可约多项式的次数（根据命题 3.117）．但如果 z_{n+1} 满足 k 上的 d 次多项式，则它在更大域 $F=k(z_1,\cdots,z_n)$ 上满足 $d'\leqslant d$ 次多项式．由此可知

$$[k(z_1,\cdots,z_{n+1}):k(z_1,\cdots,z_n)]=[F(z_{n+1}):F]\leqslant[k(z_{n+1}):k].$$

所以

$$[k(z_1,\cdots,z_{n+1}):k]=[F(z_{n+1}):k]=[F(z_{n+1}):F][F:k]$$

是有限的．

（ⅲ）现在根据（ⅱ），$k(y,z)/k$ 是有限的．因为有限维向量空间的任一子空间也是有限维的[系3.90(ⅰ)]，所以 $k(y+z)\subseteq k(y,z)$ 和 $k(yz)\subseteq k(y,z)$ 也是有限的．根据（ⅰ），$y+z$，yz 和 y^{-1} 都是 k 上的代数元素．

352

（ⅳ）立刻从（ⅲ）得出． ■

定义 给定扩张$\mathbb{C}/\mathbb{Q}$，定义**代数数**为

$$\mathbb{A}=\mathbb{C}_{\text{alg}}.$$

于是，$\mathbb{A}$ 由成为$\mathbb{Q}[x]$ 中非零多项式根的那些复数组成，命题表明$\mathbb{A}$ 是$\mathbb{C}$ 的子域，它是$\mathbb{Q}$ 上代数扩张．

例 6.55 我们断言$\mathbb{A}/\mathbb{Q}$ 是代数扩张，但不是有限的．假设有某个整数 n 使得 $[\mathbb{A}:\mathbb{Q}]=n$. 现在存在 $n+1$ 次不可约多项式 $p(x)\in\mathbb{Q}[x]$，例如取 $p(x)=x^{n+1}-2$．如果 α 是 $p(x)$ 的根，则 $\alpha\in\mathbb{A}$，从而$\mathbb{Q}(\alpha)\subseteq\mathbb{A}$. 于是，$\mathbb{A}$ 是$\mathbb{Q}$ 上的一个包含 $(n+1)$ 维子空间的 n 维向量空间，这是一个矛盾. ■

引理 6.56（ⅰ）如果 $k\subseteq K\subseteq E$ 是域塔，且 E/K 和 K/k 都是代数扩张，则 E/k 也是代数扩张．

（ⅱ）设

$$K_0\subseteq K_1\subseteq\cdots\subseteq K_n\subseteq K_{n+1}\subseteq\cdots$$

是域的升塔．如果对一切 $n\geqslant0$，K_{n+1}/K_n 都是代数扩张，则 $K^*=\bigcup_{n\geqslant0}K_n$ 是域，它在 K_0 上是代数扩张．

（ⅲ）设 $K=k(A)$，即 K 是通过在 k 中添加集合 A 的元素得到的．如果每个 $a\in A$ 都是 k 上的代数元素，则 K/k 是代数扩张．

证明（ⅰ）设 $e\in E$，因 E/K 是代数扩张，存在某个 $f(x)=\sum_{i=0}^{n}a_ix^i\in K[x]$ 以 e 为根．如果 $F=k(a_0,\cdots,a_n)$，则 e 是 F 上的代数元素，从而 $k(a_0,\cdots,a_n,e)=F(e)$ 是 F 的有限扩张；即 $[F(e):F]$ 有限．因 K/k 是代数扩张，每个 a_i 都是 k 上的代数元素，命题6.54(ⅱ)表明中间域 F 在 k 上是有限维的，即 $[F:k]$ 有限．

$$[k(a_0,\cdots,a_n,e):k]=[F(e):k]=[F(e):F][F:k]$$

有限，根据命题6.54(ⅰ)，e 是 k 上的代数元素．由此可知 K/k 是代数扩张．

（ⅱ）如果 y，$z\in K^*$，则它们在 K^* 中，因为 $y\in K_m$ 和 $z\in K_n$，可以假定 $m\leqslant n$，从而 y，$z\in K_n\subseteq K^*$．因 K_n 是域，它包含 $y+z$，yz 和 y^{-1}（如果 $y\neq0$）．所以 K^* 是域．

如果 $z\in K^*$，则必有某个 n 使得 z 在 K_n 中．而由（ⅰ）的一个显然的归纳推广可知 K_n/K_0 是代数扩张，从而 z 是 K_0 上的代数元素．因 K^* 的每个元素都是 K_0 上的代数元素，所以 K^*/K_0 是代数扩张．

（ⅲ）设 $z \in k(A)$，由习题3.95，对 z 存在一个涉及 k 和 A 中有限个元素的扩张，比如 A 的这有限个元素为 $a_1, \cdots, a_m$．因此 $z \in k(a_1, \cdots, a_m)$．根据命题6.54(ⅱ)，$k(z)/k$ 是有限的，因此 z 是 k 上的代数元素．■

353

定义 域 K 称为**代数闭的**，如果每个非常数的 $f(x) \in K[x]$ 在 K 中有根．域 k 的一个**代数闭包**是指 k 的一个代数扩张 $\overline{k}$，且 $\overline{k}$ 是代数闭的．

$\mathbb{Q}$ 的代数闭包是代数数：$\overline{\mathbb{Q}} = \mathbb{A}$. 代数基本定理说 $\mathbb{C}$ 是代数闭的，此外 $\mathbb{C}$ 是 $\mathbb{R}$ 的代数闭包．对于代数基本定理我们已经给出了一个代数证明，即定理4.49，但是这个定理的最简单的证明也许是运用复变量的刘维尔（Liouville）定理：每个有界整函数都是常数．如果 $f(x) \in \mathbb{C}[x]$ 没有根，则 $1/f(x)$ 将是一个非常数的有界整函数．

这里有两个主要的结果，第一，每个域都有一个代数闭包；第二，一个域的任意两个代数闭包同构．我们要用一个“大”多项式环来证明存在性：假定 k 是域且 T 是一个无限集合，则存在多项式环 $k[T]$，其中每个 $t \in T$ 是一个变量．（当 T 有限时，我们已经构造过 $k[T]$，无限的情形本质上是 $k[U]$ 的并，其中 U 遍历 T 的一切有限子集．对无限集 T 构造 $k[T]$ 将在习题9.93中给出）．

引理 6.57 设 k 是域，并设 $k[T]$ 是以集合 T 为变量的多项式环．如果 $t_1, \cdots, t_n \in T$ 是不同元素且 $f_i(t_i) \in k[t_i] \subseteq k[T]$ 是非常数多项式，则 $k[T]$ 中的理想 $I = (f_1(t_1), \cdots, f_n(t_n))$ 是真理想．

注 如果 $n=2$，则 $f_1(t_1)$ 和 $f_2(t_2)$ 互素，该引理说1不是它们的线性组合．

证明 如果 I 不是 $k[T]$ 中的真理想，则存在 $h_i(T) \in k[T]$ 使得

$$1 = h_1(T)f_1(t_1) + \cdots + h_n(T)f_n(t_n).$$

考虑域扩张 $k(\alpha_1, \cdots, \alpha_n)$，其中对 $i = 1, \cdots, n, \alpha_i$ 是 $f_i(t_i)$ 的根（f_i 不是常数）．记 $h_i(T)$ 中涉及的 $t_1, \cdots, t_n$ 之外的变量为 $t_{n+1}, \cdots, t_m$．赋值：$i \leqslant n$ 时，令 $t_i = \alpha_i$；$i \geqslant n+1$ 时，令 $t_i = 0$（赋值是环同态 $K[T] \to k(\alpha_1, \cdots, \alpha_n)$），右端为0，得出矛盾 $1=0$. ■

定理 6.58 给定域 k，存在 k 的代数闭包 $\overline{k}$.

证明 设 T 是集合，它和 $k[x]$ 中的非常数多项式的族构成一一对应．设 $R = k[T]$ 是大多项式环，并设 I 是 R 中由一切形如 $f(t_f)$ 的元素生成的理想，其中 $t_f \in T$；即如果

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0,$$

其中 $a_i \in k$，则

$$f(t_f) = (t_f)^n + a_{n-1}(t_f)^{n-1} + \cdots + a_0.$$

354

我们断言理想 I 是真理想．如果不是真理想，则 $1 \in I$，并存在不同的元素 $t_1, \cdots, t_n \in T$ 和多项式 $h_1(T), \cdots, h_n(T) \in k[T]$ 使得 $1 = h_1(T)f_1(t_1) + \cdots + h_n(T)f_n(t_n)$，与引理矛盾．因此根据定理6.46，存在 R 中的极大理想 M 包含 I. 定义 $K=R/M$. 现在分几步完成证明．

（ⅰ）K/k 是域扩张.

我们知道因为 M 是极大理想，所以 $K=R/M$ 是域．此外，由复合

$$k \xrightarrow{i} k[T] = R \xrightarrow{\text{自然映射}} R/M = K$$

（其中 i 是包含映射）构成的环映射 θ 不恒为0，这是因为 $1 \mapsto 1$，因此根据系3.53，θ 是单射．我们把 k 等同于 $\operatorname{im}\theta \subseteq K$.

（ⅱ）每个非常数多项式 $f(x) \in k[x]$ 在 $K[x]$ 中分裂．

根据定义，存在 $t_f \in T$ 使得 $f(t_f) \in I \subseteq M$，且陪集 $t_f + M \in R/M = K$ 是 $f(x)$ 的根．现在对次

数用归纳法可导出 $f(x)$ 在 K 上分裂．

（ⅲ）K/k 是代数扩张．

根据引理6.56(ⅲ)，只要证明每个 t_f+M 是 k 上的代数元素 [因为 $K=k(一切\ t_f+M)$]，而这是显然的，因为 t_f 是 $f(x)\in k[x]$ 的根．

显然 K 是代数闭的，但证明富于技巧 [见 I. M. Isaacs "Roots of Polynomials in Algebraic Extensions of Fields," *American Mathematical Monthly* 87 (1980)，543～544]．我们通过下列构造来避开这一证明．定义 $k_1=K$ 并迭代：按照从 k 构造 K 相同的方式，从 k_n 构造 k_{n+1}．存在一个域塔

$$k=k_0\subseteq k_1\subseteq\cdots\subseteq k_n\subseteq k_{n+1}\subseteq\cdots,$$

其中每一个扩张 k_{n+1}/k_n 都是代数的，且 $k_n[x]$ 中的每一个非常数多项式在 k_{n+1} 中都有一个根．根据引理6.56(ⅱ)，$\Omega=\bigcup_n k_n$ 是 k 的一个代数扩张．我们断言，Ω 是代数闭的．如果 $g(x)=\sum_{i=0}^{m}\omega_i x^i\in\Omega[x]$ 是一个非常数多项式，则它只有有限个系数 $\omega_0,\omega_1,\cdots,\omega_m$，因此存在某个包括所有系数的 k_q．由此可得 $g(x)\in k_q[x]$，于是如所期望的，$g(x)$ 在 $k_{q+1}\subseteq\Omega$ 中有一个根．因此，Ω 是 k 的代数闭包．■

系 6.59 *如果 k 是可数域，则它有可数的代数闭包．特别地，$\mathbb{Q}$ 或 $\mathbb{F}_p$ 有可数的代数闭包．*

证明 如果 k 是可数的，则因为 $k[x]$ 可数，所以一切非常数的多项式的集合 T 可数，比如 $T=\{t_1,t_2,\cdots\}$．因此 $k[T]=\bigcup_{\ell\geqslant 1}k[t_1,\cdots,t_\ell]$ 是可数的，它的商 k_1（定理 6.58 证明中的商）也是可数的．对 $n\geqslant 0$ 用归纳法可知每个 k_n 可数．最后，可数集的可数并也是可数的，所以 k 的代数闭包是可数的．■

我们现在证明代数闭包的唯一性．

定义 *如果 F/k 和 K/k 都是扩张，则一个 **k-映射**是指逐点固定 k 的环同态 $\varphi: F\to K$.*

我们注意到，如果 K/k 是扩张，$\varphi: K\to K$ 是 k-映射，且 $a\in K$ 是某个不可约多项式 $p(x)\in k[x]$ 的根，则 φ 置换 $p(x)$ 在 K 中的一切根 $\{a=a_1,a_2,\cdots,a_r\}$．如果 $p(x)=x^n+c_{n-1}x^{n-1}+\cdots+c_0$，则

355

$$0=p(a_i)=a_i^n+c_{n-1}a_i^{n-1}+\cdots+c_0,$$

因为 φ 固定一切 $c_i\in k$，从而

$$\begin{aligned}0&=[\varphi(a_i)]^n+\varphi(c_{n-1})[\varphi(a_i)]^{n-1}+\cdots+\varphi(c_0)\\&=[\varphi(a_i)]^n+c_{n-1}[\varphi(a_i)]^{n-1}+\cdots+c_0,\end{aligned}$$

所以 $\varphi(a_i)$ 是 $p(x)$ 在 K 中的根．最后，因 φ 是单射和 $\{a_1,a_2,\cdots,a_r\}$ 有限，所以 φ 是这些根的一个置换．

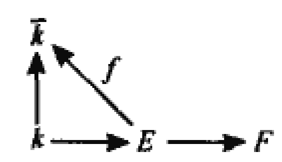
引理 6.60 *如果 K/k 是代数扩张，则每个 k-映射 $\varphi: K\to K$ 是 K 的自同构.*

证明 根据系 3.53，k-映射 φ 是单射．为证明 φ 是满射，设 $a\in K$. 因 K/k 是代数扩张，存在不可约多项式 $p(x)\in k[x]$ 以 a 为根．如同我们前面的注记，φ 是 k-映射蕴涵它置换 $p(x)$ 在 K 中的那些根的集合．因此有某个 i 使得 $a=\varphi(a_i)$，所以 $a\in\operatorname{im}\varphi$. ■

下一引理将通过把函数族排成偏序来运用佐恩引理．因一个函数本质上是一个集合，就是它的图像，所以取函数的并以获得一个上界是合理的，下面我们给出详细讨论．

引理 6.61 *如果 $\overline{k}/k$ 是代数闭包，且 F/k 是代数扩张，则存在单射 k-映射 $\psi: F\to\overline{k}$.*

证明 如果 E 是中间域，$k\subseteq E\subseteq F$，我们把一个有序对 (E,f) 称为一个"逼近"，如果 $f:E\to\overline{k}$ 是一个 k-映射. 在下图中，除 f 之外的箭头都是包含映射.



定义

$$X=\{\text{逼近}(E,f)\}.$$

注意，因为 $(k,1_k)\in X$，所以 $X\neq\varnothing$. 定义 X 上的偏序为

$$(E,f)\preceq(E',f')\ \text{如果}\ E\subseteq E'\ \text{且}\ f'\mid E=f.$$

限制 $f'\mid E$ 等于 f 的意思是指 f'扩张 f；即两个函数只要可能就是一致的：对一切 $u\in E,f'(u)=f(u)$.

易知链

$$S=\{(E_j,f_j):j\in J\}$$

的一个上界是 $(\bigcup E_j,\bigcup f_j)$. 显然$\bigcup E_j$ 是中间域. 可以把 $\Phi=\bigcup f_j$ 理解为各个 f_j的图像的并，但下面是更实际的描述：如果 $u\in\bigcup E_j$，则有某个 j_0 使得 $u\in E_{j_0}$，并有 $\Phi:u\mapsto f_{j_0}(u)$. 注意 Φ 是合理定义的：如果 $u\in E_{j_1}$，为了简化记号，可以假定 $E_{j_0}\subseteq E_{j_1}$，因为 f_{j_1}是 f_{j_0}的扩张，于是有 $f_{j_1}(u)=f_{j_0}(u)$. 读者可以验证 Φ 是 k-映射.

356

根据佐恩引理，X 中存在极大元素(E_0,f_0). 我们断言 $E_0=F$，这就完成了证明（取$\psi=f_0$ 即可）. 如果 $E_0\subsetneq F$，则有 $a\in F$ 而 $a\notin E_0$. 因 F/k 是代数扩张，所以 F/E_0 也是代数扩张，于是存在不可约多项式 $p(x)\in E_0[x]$ 以 a 为根. 因 $\overline{k}/k$ 是代数扩张且 $\overline{k}$ 是代数闭包，我们有 $\overline{k}[x]$ 中的因式分解：

$$f_0^*(p(x))=\prod_{i=1}^{n}(x-b_i),$$

其中 $f_0^*:E_0[x]\to\overline{k}[x]$ 是 f_0 诱导的映射. 如果一切 b_i 都在 $f_0(E_0)\subseteq\overline{k}$ 中，则对一切 i，$f_0^{-1}(b_i)\in E_0\subseteq F$，并存在 $p(x)$ 在 $F[x]$ 中的因式分解，它就是 $p(x)=\prod_{i=1}^{n}[x-f_0^{-1}(b_i)]$. 但 $a\notin E_0$ 蕴涵对一切 $i,a\neq f_0^{-1}(b_i)$. 由此，$x-a$ 是 $p(x)$ 在 $F[x]$ 中的另一个因式，这与唯一因子分解矛盾. 由此可知存在某个 $b_i\notin\operatorname{im}f_0$. 根据定理3.120(ii)，我们可以定义 $f_1:E_0(a)\to\overline{k}$ 为

$$c_0+c_1a+c_2a^2+\cdots\mapsto f_0(c_0)+f_0(c_1)b_i+f_0(c_2)b_i^2+\cdots.$$

容易验证 f_1 是（合理定义的）扩张 f_0 的 k-映射. 因此 $(E_0,f_0)\prec(E_0(a),f_1)$，与 (E_0,f_0) 的极大性矛盾. 这就完成了证明. ■

定理 6.62 *域 k 的任意两个代数闭包经一个 k-映射而同构.*

证明 设 K 和 L 是域k 的两个代数闭包. 根据引理 6.61，存在 k-映射$\psi:K\to L$ 和 $\theta:L\to K$. 根据引理 6.60，两个复合 $\theta\psi:K\to K$ 和 $\psi\theta:L\to L$ 都是自同构. 由此 ψ（和 θ）是 k-同构. ■

现在可以说一个域的代数闭包了.

本节剩下的内容是研究任意域的结构，我们从单超越扩张$k(x)$ 开始，其中 k 是域，x 是 k 上的超越元素，即考察函数域 $k(x)$.

定义 *如果 $\varphi\in k(x)$，则存在多项式 $g(x),h(x)\in k[x]$ 满足 $(g,h)=1$ 且 $\varphi=g(x)/h(x)$. 定*

义 φ 的**次数**[记为 degree (φ)] 为

[357]

$$\text{degree}(\varphi)=\max\{\deg(g),\deg(h)\}.$$

一个有理函数 $\varphi\in k(x)$ 叫做**线性分式变换**，如果

$$\varphi=\frac{ax+b}{cx+d},$$

其中 $a,b,c,d\in k$ 和 $ad-bc\neq 0$.

现在 $\varphi\in k(x)$ 的次数为 0 当且仅当 φ 是一个常数（即 $\varphi\in k$），而习题 6.56 说 $\varphi\in k(x)$ 的次数为 1 当且仅当 φ 是线性分式变换．如果 $A=\begin{bmatrix}a & b\\ c & d\end{bmatrix}\in \mathrm{GL}(2,k)$，记 $\langle A\rangle=(ax+b)/(cx+d)$．如果定义 $\langle A'\rangle\langle A\rangle=\langle A'A\rangle$，则容易验证一切元素在 k 中的线性分式变换的集合 LF (k) 在这个运算下是群．习题 6.57 中，读者将证明 LF $(k)\cong \mathrm{PGL}(2,k)=\mathrm{GL}(2,k)/Z(2,k)$，其中 $Z(2,k)$ 是一切 2×2（非零）标量矩阵组成的（正规）子群．

命题 6.63 *如果 $\varphi\in k(x)$ 不是常数，则 φ 是 k 上的超越元素，且 $k(x)/k(\varphi)$ 是有限扩张且*

$$[k(x):k(\varphi)]=\text{degree}(\varphi).$$

此外，如果 $\varphi=g(x)/h(x)$ 且 $(g,h)=1$，则

$$\text{irr}(x,k(\varphi))=g(y)-\varphi h(y).$$

证明 设 $g(x)=\sum a_ix^i$ 和 $h(x)=\sum b_ix^i\in k[x]$. 现在 $\theta(y)=g(y)-\varphi h(y)$ 是 $k(\varphi)[y]$ 中的多项式：

$$\theta(y)=\sum a_iy^i-\varphi\sum b_iy^i=\sum(a_i-\varphi b_i)y^i.$$

如果 $\theta(y)$ 是零多项式，则它的一切系数都是 0. 但如果 b_i 是 $h(y)$ 的一个非零系数，则 $a_i-\varphi b_i=0$ 给出 $\varphi=a_i/b_i$，与 φ 不是常数的假设，即 $\varphi\notin k$ 矛盾．由此

$$\deg(\theta)=\deg(g(y)-\varphi h(y))=\max\{\deg(g),\deg(h)\}=\text{degree}(\varphi).$$

因 x 是 $\theta(y)$ 的根，所以 x 是 $k(\varphi)$ 上的代数元素．如果 φ 是 k 上的代数元素，则 $k(\varphi)/k$ 是有限的，从而 $[k(x):k]=[k(x):k(\varphi)][k(\varphi):k]$ 有限，产生矛盾．所以 φ 是 k 上的超越元素．

我们断言 $\theta(y)$ 是 $k(\varphi)[y]$ 中的不可约多项式．如果不是，则根据高斯的系 6.27，$\theta(y)$ 在 $k(\varphi)[y]$ 中可分解．但 $\theta(y)=g(y)-\varphi h(y)$ 关于 φ 是线性的，从而系 6.37 表明 $\theta(y)$ 是不可约的．最后，因 $\deg(\theta)=\text{degree}(\varphi)$，所以有 $[k(x):k(\varphi)]=\text{degree}(\varphi)$． ■

系 6.64 *设 $\varphi\in k(x)$，其中 $k(x)$ 是域 k 上的有理函数域，则 $k(\varphi)=k(x)$ 当且仅当 φ 是线性分式变换．*

[358]

证明 根据命题 6.63，$k(\varphi)=k(x)$ 当且仅当 degree $(\varphi)=1$，即 φ 是线性分式变换． ■

系 6.65 *如果 $k(x)$ 是域 k 上的有理函数域，则*

$$\mathrm{Gal}(k(x)/k)\cong \mathrm{LF}(k),$$

LF (k) 是 k 上一切线性分式变换的群．

证明 设 $\sigma:k(x)\to k(x)$ 是 $k(x)$ 的固定 k 的自同构．现在 $\sigma:x\mapsto x^\sigma$，其中 $x^\sigma\in k(x)$，因 σ 是满射，必有 $k(x^\sigma)=k(x)$，从而根据系 6.64，x^σ 是一个线性分式变换．定义 $\gamma:\mathrm{Gal}(k(x)/k)\to$

LF(k) 为 $\gamma: \sigma \mapsto x^{\sigma}$．读者可以验证 γ 是同态（$x^{\sigma\tau} = x^{\tau}x^{\sigma}$）；因为 γ^{-1} 是这样的函数，它把任一线性分式变换 $\varphi = (ax+b)/(cx+d)$ 指派给把 x 发送到 φ 的 $k(x)$ 的自同构，所以 γ 是同构． ■

定理 6.66（吕罗特定理） *如果 $k(x)$ 是一个单超越扩张，则每个中间域 B 也是 k 的单超越扩张：存在 $\varphi \in B$ 使得 $B = k(\varphi)$．*

证明 如果 $\beta \in B$ 不是常数，则根据命题 6.63，$[k(x):k(\beta)] = [k(x):B][B:k(\beta)]$ 是有限的，因此 $[k(x):B]$ 是有限的且 x 是 B 上的代数元素．命题 6.63 的证明表明如果 $\varphi \in k(x)$，则 φ 是 $\mathrm{irr}(x, k(\varphi))$ 的一个系数，吕罗特（Lüroth）定理要证明它的逆，即证明有 $\mathrm{irr}(x,B)$ 的某个系数 φ 使得 $B = k(\varphi)$．现在

$$\mathrm{irr}(x,B) = y^n + \beta_{n-1}y^{n-1} + \cdots + \beta_0 \in B[y].$$

每个系数 $\beta_\ell \in B \subseteq k(x)$ 都是有理函数，比如说 $\beta_\ell = g_\ell(x)/h_\ell(x)$，其中 $g_\ell(x), h_\ell(x) \in k[x]$；我们可以假定每个 g_ℓ/h_ℓ 都是既约项，即 $(g_\ell, h_\ell) = 1$．用 $f(x)$ 表示 $\mathrm{lcm}\{h_0, \cdots, h_{n-1}\}$. 于是，对所有 ℓ，有 $u_\ell(x) \in k[x]$ 使得 $f(x) = u_\ell(x)h_\ell(x)$；此外，$\gcd\{u_0, \cdots, u_{n-1}\} = 1$. 我们断言

$$i(x,y) = f(x)\,\mathrm{irr}(x,B) = f(x)y^n + u_{n-1}g_{n-1}y^{n-1} + \cdots + u_0g_0 \in k[x][y]$$

是本原多项式（当然，$k[x][y] = k[x,y]$，但我们愿意把它看作系数在 $k[x]$ 中的关于 y 的多项式）．如果 $i(x,y)$ 是非本原的，则存在一个不可约的多项式 $p(x) \in k[x]$ 整除 $f(x)$ 和每一个 $u_\ell g_\ell$. 现在，对每个 ℓ 有 $f = u_\ell h_\ell$. 如果对某个 ℓ 有 $p \nmid u_\ell$，则在 $k[x]$ 中根据欧几里得引理有 $p \mid h_\ell$. 因为 $(g_\ell, h_\ell) = 1$，从而 $p \nmid g_\ell$. 但是 $p \mid u_\ell g_\ell$（$i(x,y)$ 的第 ℓ 个系数），因此由欧几里得引理可得 $p \mid u_\ell$，产生矛盾．我们得到对所有 ℓ，$p \mid u_\ell$，这与 $\gcd\{u_{n-1}, \cdots, u_0\} = 1$ 矛盾．根据引理6.24（i），$f(x)^{-1}$ 是 $\mathrm{irr}(x,B)$ 的容度．

如果记出现在一个多项式 $a(x,y)$ 中 y 的最高指数为 $\deg_y(a)$，则 $n = \deg_y(i)$；设 $m = \deg_x(i)$．因 $i(x,y) = f(x)y^n + \sum_{\ell=0}^{n-1} f(x)\beta_\ell y^\ell$，我们有 $m = \max_\ell\{\deg(f), \deg(f\beta_\ell)\}$．现在对一切 ℓ，$h_\ell(x) \mid f(x)$，从而 $\deg(h_\ell) \leqslant \deg(f) \leqslant m$［因为 $f(x)$ 是 $i(x,y)$ 的系数之一］．另外，对 $f\beta_\ell = \mathrm{lcm}\{h_0, \cdots, h_{n-1}\}g_\ell/h_\ell = (\mathrm{lcm}\{h_0, \cdots, h_{n-1}\}/h_\ell)g_\ell \in k[x]$，有 $\deg(g_\ell) \leqslant \deg(u_\ell g_\ell) = \deg(f\beta_\ell) \leqslant m$．由此可知 $\deg(g_\ell) \leqslant m$ 和 $\deg(h_\ell) \leqslant m$. 359

$\mathrm{irr}(x,B)$ 有某个系数 β_j 不是常数，否则 x 是 k 上的代数元素．省略下标 j，记 $\beta_j = g(x)/h(x)$，并定义

$$\varphi = \beta_j = g(x)/h(x) \in B.$$

现在 $g(y) - \varphi h(y) = g(y) - g(x)h(x)^{-1}h(y) \in B[y]$ 以 x 为根，从而 $\mathrm{irr}(x,B)$ 在 $B[y] \subseteq k(x)[y]$ 中整除 $g(y) - \varphi h(y)$．所以存在 $q(x,y) \in k(x)[y]$ 使得

$$\mathrm{irr}(x,B)q(x,y) = g(y) - \varphi h(y). \tag{1}$$

因 $g(y) - \varphi h(y) = h(x)^{-1}(h(x)g(y) - g(x)h(y))$，所以容度 $c(g(y) - \varphi h(y))$ 是 $h(x)^{-1}$ 且相伴本原多项式是

$$\Phi(x,y) = h(x)g(y) - g(x)h(y).$$

注意 $\Phi(x,y) \in k[x][y]$ 和 $\Phi(y,x) = -\Phi(x,y)$．

重写等式(1)，其中 $c(q) \in k(x)$ 是 $q(x,y)$ 的容度：

$$f(x)^{-1}i(x,y)c(q)q(x,y)^{*}h(x) = \Phi(x,y)$$

（回忆 $f(x)^{-1}$ 是 $\mathrm{irr}(x,B)$ 的容度且 $i(x,y)$ 是它的相伴本原多项式）．根据高斯引理 6.23，积

$i(x,y)q(x,y)$*是本原的．但 $\Phi(x,y)\in k[x][y]$，从而引理6.24(ⅲ)给出 $f(x)^{-1}c(q)h(x)\in k[x]$．现在定义 $q^{**}(x,y)=f(x)^{-1}c(q)h(x)q(x,y)$，从而 $q^{**}(x,y)\in k[x,y]$ 且在 $k[x,y]$ 中有

$$i(x,y)q^{**}(x,y)=\Phi(x,y). \tag{2}$$

我们计算(2)式中的次数：左端关于 x 的次数是

$$\deg_x(iq^{**})=\deg_x(i)+\deg_x(q^{**})=m+\deg_x(q^{**}), \tag{3}$$

而右端关于 x 的次数是

$$\deg_x(\Phi)=\max\{\deg(g),\deg(h)\}\leqslant m, \tag{4}$$

如同上面我们知道的那样．由此可知 $m+\deg_x(q^{**})\leqslant m$，从而 $\deg_x(q^{**})=0$；即 $q^{**}(x,y)$ 是一个变量 y 的函数．但 $\Phi(x,y)$ 是关于 x 的本原多项式，因此对称 $\Phi(y,x)=-\Phi(x,y)$ 表明它也是关于 y 的本原多项式．于是 q^{**} 是一个常数，从而 $i(x,y)$ 和 $\Phi(x,y)$ 在 $k[x,y]$ 中相伴；因此 $\deg_x(\Phi)=\deg_x(i)=m$. 这个等式和等式 (4) 一起给出

$$m=\deg_x(\Phi)=\max\{\deg(g),\deg(h)\}.$$

Φ 的对称性又给出 $\deg_y(\Phi)=\deg_x(\Phi)$，从而

$$n=\deg_y(\Phi)=\deg_x(\Phi)=m=\max\{\deg(g),\deg(h)\}.$$

根据定义，$\text{degree}(\varphi)=\max\{\deg(g),\deg(h)\}=m$，因此命题 6.63 给出 $[k(x):k(\varphi)]=m$．最后，因 $\varphi\in B$，有 $[k(x):k(\varphi)]=[k(x):B][B:k(\varphi)]$．由于 $[k(x):B]=n=m$，因此这迫使 $[B:k(\varphi)]=1$；即 $B=k(\varphi)$． ■

对 $n>1$，有满足 $k\subseteq B\subseteq k(x_1,\cdots,x_n)$ 的中间域 B 的例子，它不是这样容易描述的．

360

我们现在考虑更一般的域扩张．

定义 *设 E/k 是域扩张．E 的子集 U 称为在 k 上* **代数相关**，*如果存在有限子集 $\{u_1,\cdots,u_n\}\subseteq U$ 和非零多项式 $f(x_1,\cdots,x_n)\in k[x_1,\cdots,x_n]$ 使得 $f(u_1,\cdots,u_n)=0$．称 E 的子集 B* **代数无关**，*如果它不是代数相关的．*

设 E/k 是域扩张，设 $u_1,\cdots,u_n\in E$，并设 $\varphi:k[x_1,\cdots,x_n]\to E$ 是赋值映射，即对一切 $f(x_1,\cdots,x_n)\in k[x_1,\cdots,x_n]$，$\varphi$ 是把 $f(x_1,\cdots,x_n)$ 发送到 $f(u_1,\cdots,u_n)$ 的同态．现在 $\{u_1,\cdots,u_n\}$ 是代数相关的当且仅当 $\ker\varphi\neq\{0\}$．如果 $\{u_1,\cdots,u_n\}$ 是代数无关的，则 φ 扩张为同构 $k(x_1,\cdots,x_n)\cong k(u_1,\cdots,u_n)\subseteq E$，其中 $k(x_1,\cdots,x_n)$ 是有理函数 $\text{Frac}(k[x_1,\cdots,x_n])$ 的域．特别地，$\{x_1,\cdots,x_n\}\subseteq E=k(x_1,\cdots,x_n)$ 是代数无关的，这是因为在该情形下，φ 是恒等映射．

因代数相关子集必须是非空的，由此空子集 $\varnothing$ 是代数无关的．单元集 $\{e\}\subseteq E$ 是代数相关的如果 e 是 k 上的代数元素，即 e 是 k 上一个非常数多项式的根，而 e 是代数无关的，如果 e 是 k 上的一个超越元素，此时 $k(e)\cong k(x)$．

命题 6.67 *设 E/k 是域扩张，并设 $U\subseteq E$，则 U 在 k 上是代数相关的当且仅当存在 $u\in U$ 使得 u 是 $k(U-\{u\})$ 上的代数元素．*

证明 如果 U 在 k 上代数相关，则存在代数相关的有限子集 $U'=\{u_1,\cdots,u_n\}\subseteq U$．对 $n\geqslant1$ 用归纳法证明有某个 u_i 是 $k(U'-\{u_i\})$ 上的代数元素．如果 $n=1$，则存在某个非零多项式 $f(x)\in k[x]$ 使得 $f(u_1)=0$，即 u_1 是 k 上的代数元素．而 $U'-\{u_1\}=\varnothing$，所以 u_1 是 $k(U'-\{u_1\})=k(\varnothing)=k$ 上的代数元素．关于归纳步，设 $U'=\{u_1,\cdots,u_{n+1}\}$ 是代数相关的．可以假定 $\{u_1,\cdots,u_n\}$ 是代数无关的，否则，归纳假设给出某个 u_j，其中 $1\leqslant j\leqslant n$，它是 $k(u_1,\cdots,\hat{u}_j,\cdots,u_n)$ 上的代数元

素，因此是$k(U'-\{u_j\})$上的代数元素．因U'是代数相关的，存在非零多项式$f(X,y)\in k[x_1,\cdots,x_n,y]$使得$f(\vec{u},u_{n+1})=0$，其中$X=(x_1,\cdots,x_n)$，$y$是新变量，$\vec{u}=(u_1,\cdots,u_n)$．可以写$f(X,y)=\sum_i g_i(X)y^i$，其中$g_i(X)\in k[X]$（因为$k[X,y]=k[X][y]$）．因$f(X,y)\neq 0$，有某个$g_i(X)\neq 0$，由此从$\{u_1,\cdots,u_n\}$的代数无关性可知$g_i(\vec{u})\neq 0$．所以$h(y)=\sum_i g_i(\vec{u})y^i\in k(U)[y]$不是零多项式．但$0=f(\vec{u},u_{n+1})=h(u_{n+1})$，从而$u_{n+1}$是$k(u_1,\cdots,u_n)$上的代数元素．

反之，假定u是$k(U-\{u\})$上的代数元素，可以假定$U-\{u\}$是有限的，比如$U-\{u\}=\{u_1,\cdots,u_n\}$，其中$n\geqslant 0$（如果$n=0$，我们指的是$U-\{u\}=\varnothing$）．对$n\geqslant 0$用归纳法证明$U$是代数相关的．如果$n=0$，则$u$是$k$上的代数元素，因此$\{u\}$是代数相关的．关于归纳步，设$U-\{u_{n+1}\}=\{u_1,\cdots,u_n\}$．可以假定$U-\{u_{n+1}\}=\{u_1,\cdots,u_n\}$代数无关，否则$U-\{u_{n+1}\}$，并因此它的超集$U$是代数相关的．根据假设，存在非零多项式$f(y)=\sum_i c_iy^i\in k(u_1,\cdots,u_n)[y]$使得$f(u_{n+1})=0$．因$f(y)\neq 0$，可以假定它有一项，比如$c_j\neq 0$．现在对每个$i$，$c_i\in k(u_1,\cdots,u_n)$，从而存在有理函数$c_i(x_1,\cdots,x_n)$使得$c_i(\vec{u})=c_i$，其中$\vec{u}=(u_1,\cdots,u_n)$．因$f(u_{n+1})=0$，我们可以通分，从而可假定每个$c_i(x_1,\cdots,x_n)$是$k[x_1,\cdots,x_n]$中的多项式．此外，$c_j(\vec{u})\neq 0$蕴涵$c_j(x_1,\cdots,x_n)\neq 0$，从而 [361]

$$g(x_1,\cdots,y)=\sum_i c_i(x_1,\cdots,x_n)y^i$$

非零．所以$\{u_1,\cdots,u_{n+1}\}$代数相关． ■

定义 域扩张E/k称为**纯超越**的，如果不是$E=k$就是E包含一个代数无关的子集B且$E=k(B)$．

如果$X=\{x_1,\cdots,x_n\}$是有限集，则

$$k(X)=k(x_1,\cdots,x_n)=\mathrm{Frac}(k[x_1,\cdots,x_n])$$

叫做n个变量的**函数域**.

我们要证明如果E/k是域扩张，则存在中间域F使得F/k是纯超越的以及E/F是代数的．事实上，$F=k(B)$，其中B是E/k的极大代数无关子集，而且任意两个这样的子集有相同的基数．这个证明本质上和向量空间的维数不变性的证明相同，因此我们把这个证明公理化．

回忆从集合Y到集合Z的一个关系是子集$R\subseteq Y\times Z$．我们写作yRz代替$(y,z)\in R$．特别地，如果Ω是一个集合，$\mathcal{P}(\Omega)$是它的一切子集的族，$\preceq$是从Ω到$\mathcal{P}(\Omega)$的一个关系，则我们用

$$x\preceq S$$

代替$(x,S)\in\preceq$．

定义 集合Ω上的一个**相关关系**是指从Ω到$\mathcal{P}(\Omega)$的关系$\preceq$，它满足下列公理：

（i）如果$x\in S$，则$x\preceq S$；

（ii）如果$x\preceq S$，则存在有限子集$S'\subseteq S$使得$x\preceq S'$；

（iii）**（传递性）** 如果$x\preceq S$，且有某个$T\subseteq\Omega$满足对一切$s\in S, s\preceq T$，则$x\preceq T$；

（iv）**（交换公理）** 如果$x\preceq S$和$x\not\preceq S-\{y\}$，则$y\preceq(S-\{y\})\cup\{x\}$．

传递公理说，如果x和集合S相关，且S的每个元素和另一个集合T相关，则x和T相关．

例 6.68 如果Ω是向量空间，则定义$x\preceq S$为$x\in\langle S\rangle$，这是由S张成的子空间．我们断言$\preceq$是相关关系．前三个公理容易验证．我们验证交换公理．如果$x\preceq S$且$x\not\preceq S-\{y\}$，则$S=S'\cup\{y\}$，其中$y\notin S'$．存在标量a_i,a使得$x=ay+\sum_i a_is_i$，其中$s_i\in S'$，因$x\notin\langle S'\rangle$，必有$a\neq 0$．所以

362 $y=a^{-1}(x-\sum_i a_i s_i)\in\langle S',x\rangle$，从而 $y\preceq S'\cup\{x\}$. ■

引理 6.69 如果 E/k 是域扩张，定义 $\alpha\preceq S$ 为 α 是 $k(S)$ 上的代数元素，则 $\alpha\preceq S$ 是一个相关关系.

证明 容易验证相关关系定义中的前两条公理，现在我们验证公理（ⅲ）：如果 $x\preceq S$ 且有某个 $T\subseteq\Omega$ 满足对一切 $s\in S$ 有 $s\preceq T$，则 $x\preceq T$. 如果 F 是一个中间域，用 $\overline{F}$ 表示 F 上一切代数元素 $e\in E$ 组成的域. 使用这个记号，$x\preceq S$ 当且仅当 $x\in\overline{k(S)}$. 此外，对一切 $s\in S$ 有 $s\preceq T$ 就是说 $S\subseteq\overline{k(T)}$，由此，根据引理6.56(ⅰ)，$x\in\overline{k(T)}$，从而 $x\preceq T$.

交换公理说，如果 $u\preceq S$ 且 $u\not\preceq S-\{v\}$，则 $v\preceq(S-\{v\})\cup\{u\}$. 记 $S'=S-\{v\}$，于是 u 是 $k(S)$ 上的代数元素，且 u 是 $k(S')$ 上的超越元素. 现在根据命题6.67，$\{u,v\}$ 在 $k(S')$ 上是代数相关的，从而存在非零多项式 $f(x,y)\in k(S')[x,y]$ 使得 $f(u,v)=0$. 更详细地说，$f(x,y)=g_0(x)+g_1(x)y+\cdots+g_n(x)y^n$，其中 $g_n(x)$ 非零. 因 u 是 $k(S')$ 上的超越元素，必有 $g_n(u)\neq 0$. 所以 $h(y)=f(u,y)\in k(S',u)[y]$ 是非零多项式. 但 $h(v)=f(u,v)=0$，因此 v 是 $k(S',u)$ 上的代数元素，即 $v\preceq S'\cup\{u\}=(S-\{v\})\cup\{u\}$. ■

例 6.68 引出下面的术语.

定义 设 $\preceq$ 是集合 Ω 上的相关关系. 子集 $S\subseteq\Omega$ 称为**相关的**，如果存在 $s\in S$ 使得 $s\preceq S-\{s\}$；称 S 是**无关的**，如果它不是相关的. 我们说子集 S **生成** Ω，如果对一切 $x\in\Omega$ 有 $x\preceq S$. Ω 的一个**基**是指生成 Ω 的无关子集.

注意 $\varnothing$ 是无关的，因为相关子集有元素. 如果 $S\neq\varnothing$，则 S 是无关的当且仅当对一切 $s\in S$ 有 $s\not\preceq S-\{s\}$. 由此，无关集的每个子集也是无关的. 根据命题 6.67，在引理 6.69 中的相关关系下，刚定义的无关和前面定义的代数无关是一致的.

引理 6.70 设 $\preceq$ 是集合 Ω 上的相关关系. 如果 $T\subseteq\Omega$ 是无关的且有某个 $z\in\Omega$ 满足 $z\not\preceq T$，则 $T\cup\{z\}\supsetneq T$ 是严格较大的无关子集.

证明 因 $z\not\preceq T$，公理（ⅰ）给出 $z\notin T$，从而 $T\subsetneq T\cup\{z\}$，由此 $(T\cup\{z\})-\{z\}=T$. 如果 $T\cup\{z\}$ 是相关的，则存在 $t\in T\cup\{z\}$ 使得 $t\preceq(T\cup\{z\})-\{t\}$. 如果 $t=z$，则 $z\preceq T\cup\{z\}-\{z\}=T$，和 $z\not\preceq T$ 矛盾. 所以 $t\in T$. 因 T 是无关的，$t\not\preceq T-\{t\}$. 如果在交换公理中令 $S=T\cup\{z\}-\{t\}$，$t=x$ 和 $y=z$，则有 $z\preceq(T\cup\{z\}-\{t\})-\{z\}\cup\{t\}=T$，和假设 $z\not\preceq T$ 矛盾. 所以 $T\cup\{z\}$ 无关. ■

我们现在推广交换引理，即引理 3.84 的证明和它在维数不变性上的应用（即定理 3.85).

定理 6.71 如果 $\preceq$ 是集合 Ω 上的相关关系，则 Ω 有基. 事实上，Ω 的每个无关子集 B 都是一个基的一部分.

363 **证明** 因空集 $\varnothing$ 是无关的，所以第二个陈述蕴涵第一个陈述.

我们用佐恩引理证明存在 Ω 的包含 B 的极大无关子集. 设 X 是 Ω 的包含 B 的一切无关子集的族，用包含作为偏序. 注意 X 非空，因为 $B\in X$. 假设 $\mathcal{C}$ 是 X 中的链. 显然，如果 $C^*=\bigcup_{C\in\mathcal{C}}C$ 在 X 中，即 C^* 是无关的，则 C^* 是 $\mathcal{C}$ 的一个上界. 如果相反，C^* 是相关的，则存在 $y\in C^*$ 使得 $y\preceq C^*-\{y\}$. 根据公理（ⅱ），存在有限子集 $\{x_1,\cdots,x_n\}\subseteq C^*-\{y\}$ 使得 $y\preceq\{x_1,\cdots,x_n\}-\{y\}$. 现在有 $C_0\in\mathcal{C}$ 使得 $y\in C_0$，且对每个 i，存在 $C_i\in\mathcal{C}$ 使得 $x_i\in C_i$. 因 $\mathcal{C}$ 是链，它们中有一个（把它叫做 C'）包含其他各个，且相关集合 $\{y,x_1,\cdots,x_n\}$ 包含在 C' 中. 但因 C' 是无关的，从而它的子集也是无关的，于是出现矛盾. 现在佐恩引理给出 X 的极大元素 M，即 M 是 Ω 的包含 B 的极大无关

子集．如果 M 不是基，则存在 $x \in \Omega$ 使得 $x \not\preceq M$．根据引理6.70，$M \cup \{x\}$ 是严格大于 M 的无关集，这和 M 的极大性矛盾．所以基存在． ■

定理 6.72 如果 Ω 是有相关关系 $\preceq$ 的集合，则任意两个基 B 和 C 有相同的基数．

证明 如果 $B=\varnothing$，我们断言 $C=\varnothing$．否则，存在 $y \in C$，因 C 是无关的，所以 $y \not\preceq C-\{y\}$．但 $y \preceq B=\varnothing$ 且 $\varnothing \subseteq C-\{y\}$，因此公理(ⅲ)给出 $y \preceq C-\{y\}$，于是出现矛盾．所以可以假定 B 和 C 两者都非空．

现在假定 B 是有限集，比如 $B=\{x_1,\cdots,x_n\}$．对 $k \geqslant 0$ 用归纳法证明存在 $\{y_1,\cdots,y_{k-1}\} \subseteq C$ 使得

$$B_k=\{y_1,\cdots,y_{k-1},x_k,\cdots,x_n\}$$

是基：B 中元素 $x_1,\cdots,x_{k-1}$ 可以换成元素 $y_1,\cdots,y_{k-1} \in C$ 使得 B_k 成为基．定义 $B_0=B$，基础步的意思是：如果 B 的元素没有被替换，则 $B=B_0$ 是基，这是显然成立的．关于归纳步，假定 $B_k=\{y_1,\cdots,y_{k-1},x_k,\cdots,x_n\}$ 是基．我们断言存在 $y \in C$ 满足 $y \not\preceq B_k-\{x_k\}$．否则对一切 $y \in C$ 有 $y \preceq B_k-\{x_k\}$．但因 C 是基，所以 $x_k \preceq C$，从而公理(ⅲ)给出 $x_k \preceq B_k-\{x_k\}$，和 B_k 是无关的相矛盾．因此可以选取 $y_k \in C$ 使得 $y_k \not\preceq B_k-\{x_k\}$．根据引理 6.70，由

$$B_{k+1}=(B_k-\{x_k\}) \cup \{y_k\}=\{y_1,\cdots,y_k,x_{k+1},\cdots,x_n\}$$

定义的集合 B_{k+1} 是无关的．为证明 B_{k+1} 是基，只要证明它生成 Ω. 现在 $y_k \preceq B_k$（因为 B_k 是基），且 $y_k \not\preceq B_k-\{x_k\}$，交换公理给出 $x_k \preceq (B_k-\{x_k\}) \cup \{y_k\}=B_{k+1}$．根据公理(ⅰ)，$B_k$ 的其他一切元素和 B_{k+1} 相关．现在 Ω 的每个元素和 B_k 相关，而 B_k 的每个元素和 B_{k+1} 相关，由公理(ⅲ)，B_{k+1} 生成 Ω.

如果 $|C|>n=|B|$，即如果 y 的个数比 x 的个数多，则 $B_n \subsetneq C$．于是 C 的一个真子集生成 Ω，和 C 的无关性矛盾．所以 $|C| \leqslant |B|$．由此 C 是有限的，从而可以交换 B 和 C 的角色而重复前面的论证．因此 $|B| \leqslant |C|$，且由此可知，如果 Ω 有有限基，则 $|B|=|C|$． 364

当 B 无限时，读者可以修改定理 6.51 的证明来完成本证明．特别地，在证明中可以在相关关系的定义中用公理(ⅱ)来替换 $\mathrm{supp}(v)$． ■

我们现在运用这个一般结果到代数相关上．

定义 如果 E/k 是域扩张，则一个**超越基** B 是指 E 在 k 上的一个极大代数无关子集，E/k 的**超越次数**定义为

$$\mathrm{tr.deg}(E/k)=|B|.$$

下一定理证明超越次数是合理定义的．

定理 6.73 如果 E/k 是域扩张，则存在超越基 B．如果 $F=k(B)$，则 F/k 是纯超越扩张且 E/F 是代数扩张．此外，如果 B 和 C 都是极大代数无关子集，则 $|B|=|C|$．

证明 在引理 6.69 中，我们知道如果定义 $\alpha \preceq S$ 为 α 是 $k(S)$ 上的代数元素，则 $\alpha \preceq S$ 是一个相关关系．根据定理 6.71 和 6.72，超越基存在，且任两个基有相同的基数，即超越次数是合理定义的．剩下的是证明如果 B 是超越基，则 $E/k(B)$ 是代数扩张．如果不是，则存在 $\alpha \in E$ 使得 α 是 $k(B)$ 上的超越元素．根据引理 6.70，$B \cup \{\alpha\}$ 是代数无关的，和 B 的极大性矛盾． ■

例 6.74 (ⅰ) 如定理 6.73 中所述，中间域 F 未必唯一．例如如果 $E=\mathbb{Q}(\pi)$，则 $\mathbb{Q}(\pi^4)$ 和 $\mathbb{Q}(\pi^2)$ 都是这样的中间域．

(ⅱ) 如果 $E=k(x_1,\cdots,x_n)$ 是域 k 上 n 个变量的有理函数域，则 $\mathrm{tr.deg}(E/k)=n$，因为 $\{x_1,\cdots,$

$x_n\}$ 是 E 的一个超越基.

(iii) 如果 E/k 是域扩张，则 E/k 是代数扩张当且仅当 $\text{tr. deg}(E/k) = 0$. ■

下面是超越次数的一个小应用.

命题 6.75 *存在不同构的域，其中每一个域同构于另一个的子域.*

证明 显然，$\mathbb{C}$ 同构于 $\mathbb{C}(x)$ 的子域. 然而，我们断言 $\mathbb{C}(x)$ 同构于 $\mathbb{C}$ 的子域. 设 B 是 $\mathbb{C}$ 在 $\mathbb{Q}$ 上的超越基，并丢弃 B 中一个元素，比如 b. $\mathbb{Q}(B-\{b\})$ 的代数闭包 F 是 $\mathbb{C}$ 的真子域，这是因为 $b \notin F$，事实上，根据命题 6.67，b 是 F 上的超越元素. 由此，根据习题 6.54，$F \cong \mathbb{C}$，从而 $F(b) \cong \mathbb{C}(x)$. 所以 $\mathbb{C}$ 和 $\mathbb{C}(x)$ 的每一个都同构于另一个的子域. 另一方面，因为 $\mathbb{C}(x)$ 不是代数闭的，所以 $\mathbb{C}(x) \not\cong \mathbb{C}$. ■

我们更详细地考虑可分性，以此继续域的结构的研究. 回忆如果 E/k 是域扩张，则元素 $\alpha \in E$ 在 k 上可分是指 α 是 k 上的超越元素或 $\text{irr}(\alpha,k)$ 是可分多项式[⊖]，即 $\text{irr}(\alpha,k)$ 无重根. 扩张 E/k 是可分的如果每个 $\alpha \in E$ 在 k 上可分，否则它是不可分的.

365

命题 6.76 *设 $f(x) \in k[x]$，其中 k 是域，并设 $f'(x)$ 是它的导数.*

(i) $f(x)$ 有重根当且仅当 $(f,f') \neq 1$.

(ii) 如果 k 是特征 $p>0$ 的域，则 $f'(x) = 0$ 当且仅当 $f(x) \in k[x^p]$.

(iii) 如果 k 是特征 $p>0$ 的域且 $f'(x)=0$，则 $f(x)$ 无重根. 反之，如果 $f(x)$ 是 $k[x]$ 中的不可约多项式，则 (i) 和 (ii) 中的条件等价.

证明 (i) 如果 $f(x)$ 有重根，则在 $k[x]$ 中 $f(x) = (x-\alpha)^2 g(x)$，从而 $f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x)$. 所以 $x-\alpha$ 是 $f(x)$ 和 $f'(x)$ 的公因式，因此 $(f,f') \neq 1$.

反之，根据系 3.41，只需在 $f(x)$ 的一个分裂域上进行证明. 如果 $x-\alpha$ 是 (f,f') 的因式，则 $f(x) = (x-\alpha)u(x)$ 和 $f'(x) = (x-\alpha)v(x)$. 乘积法则给出 $f'(x) = u(x) + (x-\alpha)u'(x)$，因此 $u(x) = (x-\alpha)(v(x)-u'(x))$. 所以

$$f(x) = (x-\alpha)u(x) = (x-\alpha)^2(v(x)-u'(x)),$$

从而 $f(x)$ 有重根.

(ii) 假定 $f(x) = \sum_i a_i x^i$ 和 $f'(x) = 0 = \sum_i i a_i x^{i-1}$. 如果系数 $a_i \neq 0$，则 $i a_i x^{i-1} = 0$ 当且仅当 $i a_i = 0$，只有 $p \mid i$ 时发生这种情形. 所以 $f(x)$ 的非零系数只有满足 $p \mid i$ 的那些 a_i，即 $f(x) \in k[x^p]$.

如果 $f(x) \in k[x^p]$，则 $f(x) = \sum_j a_{pj} x^{pj}$，$f'(x) = \sum_j pj a_{pj} x^{pj-1} = 0$.

(iii) 如果 $f'(x) = 0$，则 $(f,f') = (f,0) = f$；因此，如果 $f(x)$ 不是常数 [特别地，如果 $f(x)$ 是不可约的]，则 $(f,f') \neq 1$.

反之，如果 $f(x)$ 是不可约的，则 $(f,f') = 1$ 或 $(f,f') = f$. 现在 $(f,f') \neq 1$，从而 $(f,f') = f$，因此 $f \mid f'$. 我们断言 $f'(x) = 0$. 如果相反，$f'(x) \neq 0$，则 $f'(x)$ 有次数且 $\deg(f') < \deg(f)$. 但 $f \mid f'$ 蕴涵 $\deg(f) \leqslant \deg(f')$，这是一个矛盾. 因此 $f'(x) = 0$. ■

系 6.77 *如果 k 是特征 $p>0$ 的域且 $f(x) \in k[x]$，则存在 $e \geqslant 0$ 和多项式 $g(x) \in k[x]$ 使得 $g(x) \notin k[x^p]$ 和 $f(x) = g(x^{p^e})$. 此外，如果 $f(x)$ 是不可约的，则 $g(x)$ 是可分的.*

证明 如果 $f(x) \notin k[x^p]$，则定义 $g(x) = f(x)$. 如果 $f(x) \in k[x^p]$，则存在 $f_1(x) \in k[x]$ 使得 $f(x) = f_1(x^p)$. 注意 $\deg(f) = p\deg(f_1)$. 如果 $f_1(x) \notin k[x^p]$，定义 $g(x) = f_1(x)$. 否则，

⊖ 回忆一个不可约多项式是可分的，如果它没有重根；一个任意多项式是可分的，如果它的每个不可约因式都没有重根.

存在 $f_2(x) \in k[x]$ 使得 $f_1(x) = f_2(x^p)$，即

366

$$f(x) = f_1(x^p) = f_2(x^{p^2}).$$

因 $\deg(f) > \deg(f_1) > \cdots$，这个迭代过程经有限的 e 步之后必终止．于是 $f(x) = g(x^{p^e})$，其中 $g(x)$ 定义为 $g(x) = f_e(x)$，它不在 $k[x^p]$ 中．现在如果 $f(x)$ 是不可约的，则 $f_1(x)$ 也是不可约的，这是因为 $f_1(x)$ 的一个因式分解会产生 $f(x)$ 的一个因式分解．由此对一切 i，$f_i(x)$ 都是不可约的．特别地，$f_e(x)$ 是不可约的，从而根据命题6.76(ⅲ)，$f_e(x)$ 是可分的． ■

定义 设 k 是特征 $p>0$ 的域，并设 $f(x) \in k[x]$．如果 $f(x) = g(x^{p^e})$，其中 $g(x) \in k[x]$ 但 $g(x) \notin k[x^p]$，则

$$\deg(f) = p^e \deg(g).$$

我们称 p^e 为 $f(x)$ 的**不可分次数**，称 $\deg(g)$ 为 $f(x)$ 的**约化次数**.

例 6.78 设 $f(x) = x^{p^3} + x^p + t \in \mathbb{F}_p(t)[x]$．如果 $g(x) = x^{p^2} + x + t$，则 $g(x)$ 是可分的（因为 $g'(x) = 1 \neq 0$）．所以 $f(x)$ 的不可分次数为 p，约化次数为 p^2． ■

如果 k 是特征为素数 $p>0$ 的域，则由 $F: \alpha \mapsto \alpha^p$ 定义的弗罗贝尼乌斯（Frobenius）映射 $F: k \to k$ 是同态［因为 $(\alpha+\beta)^p = \alpha^p + \beta^p$］．和任意域同态一样，$F$ 是单射．记 $\mathrm{im}F$ 为 k^p，由此 k^p 是由 k 中一切元素的 p 次幂组成的 k 的子域：

$$k^p = \mathrm{im}\, F = \{a^p : a \in k\}.$$

说 F 是满射，即 $k = k^p$，等于说 k 中每个元素有一个 p 次根在 k 中．

定义 域 k 称为**完满域**，如果 k 有特征 0 或 k 有特征 $p>0$ 且 $k = k^p$．

k 中 p 次根的存在性与可分性密切相关．

命题 6.79 （ⅰ）域 k 是完满的当且仅当 $k[x]$ 中的每个多项式都是可分的．

（ⅱ）如果 k 是完满域，则每个代数扩张 E/k 都是可分扩张．

（ⅲ）每个有限域 k 都是完满的，且每个代数扩张 E/k 都是可分的．特别地，如果 $\overline{\mathbb{F}}_p$ 是 $\mathbb{F}_p$ 的代数闭包，则 $\overline{\mathbb{F}}_p/\mathbb{F}_p$ 是可分扩张．

证明 (ⅰ) 如果 k 有特征 0，则引理 4.4 表明 $k[x]$ 中的每个多项式都是可分的．现在假定 k 有特征 $p>0$，且 $f(x) \in k[x]$ 是不可分的．根据命题 6.76，$f(x) \in k[x^p]$，因此 $f(x) = \sum_i a_i x^{pi}$．如果 k 中每个元素都有一个 p 次根，则 $a_i = b_i^p$，其中 $b_i \in k$．因此

$$f(x) = \sum_i b_i^p x^{pi} = \left(\sum_i b_i x^i\right)^p,$$

367

从而 $f(x)$ 不是不可约的．换句话说，如果 $k = k^p$，则 $k[x]$ 中的每个不可约多项式都是可分的，因此每个多项式都是可分的．

反之，假定 $k[x]$ 中的每个多项式都是可分的．如果 k 有特征 0，则结论已经成立．如果 k 有特征 $p>0$ 且 $a \in k$，则 $x^p - a$ 有重根．因假设说不可约多项式是可分的，因此 $x^p - a$ 可分解．现在命题 3.126 说 a 在 k 中有 p 次根，即 $a \in k^p$．所以 $k = k^p$，因而 k 是完满的．

（ⅱ）如果 E/k 是代数扩张，则每个 $\alpha \in E$ 有极小多项式 $\mathrm{irr}(\alpha, k)$，根据（ⅰ），$\mathrm{irr}(\alpha, k)$ 是可分多项式，因此 α 在 k 上可分，从而 E/k 是可分扩张．

（ⅲ）和域上的任意同态一样，弗罗贝尼乌斯 $F: k \to k$ 是单射．如果 k 是特征 $p>0$ 的有限域，则习题 1.58 表明 F 必定也是满射，即 $k = k^p$．所以 k 是完满的，（ⅱ）给出剩下的陈述． ■

我们马上要用到另一种形式的命题 3.126.

引理 6.80 设 p 是素数，$e\geqslant 0$，并设 k 是特征 $p>0$ 的域．如果 $c\in k$ 且 $c\notin k^p$，则 $f(x)=x^{p^e}-c$ 在 $k[x]$ 中不可约．

证明 对 $e\geqslant 0$ 用归纳法证明，基础步成立是因为每个线性多项式是不可约的．关于归纳步，假设该陈述不成立．设 $g(x)\in k[x]$ 是不可约的，并设 $g(x)^m$（其中 $m\geqslant 1$）是能够整除 $f(x)$ 的 $g(x)$ 的最高幂：

$$x^{p^e}-c=g(x)^m h(x),$$

其中 $(g(x),h(x))=1$．取导数，$0=mg(x)^{m-1}g'(x)h(x)+g(x)^m h'(x)$，除以 $g(x)^{m-1}$，

$$0=mg'(x)h(x)+g(x)h'(x).$$

因为 $(g,h)=1$，所以 $h(x)\mid h'(x)$．如果 $h'(x)\neq 0$，则 $\deg(h')$ 有定义且 $\deg(h')<\deg(h)$，这是一个矛盾．于是 $h'(x)=0$．命题 6.76 给出

$$h(x)=h_1(x^p)，其中 h_1(x)\in k[x].$$

现在因为 $h(x)\neq 0$，所以 $mg'(x)h(x)=0$ 给出

$$mg'(x)=0 \tag{5}$$

这蕴涵 $(g^m(x))'=0$．因此命题 6.76 给出

$$g^m(x)=g_1(x^p)，其中 g_1(x)\in k[x].$$

所以，

368

$$x^{p^e}-c=g(x)^m h(x)=g_1(x^p)h_1(x^p),$$

用 x 替换 x^p 得

$$x^{p^{e-1}}-c=g_1(x)h_1(x).$$

根据归纳假设，因为 $x^{p^{e-1}}-c$ 是不可约的，所以 g_1,h_1 之一必是常数．而如果 $g_1(x)$ 是常数，则 $g_1(x^p)$ 是常数且 $g^m(x)$ 是常数，这就产生矛盾．所以 $h_1(x)$ 是常数，把它吸收进 $g_1(x)$，有 $x^{p^{e-1}}-c=g_1(x)$ 和

$$x^{p^e}-c=g_1(x^p)=g(x)^m.$$

如果 $p\mid m$，则 $x^{p^e}-c=(g(x)^p)^{m/p}$，从而所有的系数都在 k^p 中，和 $c\notin k^p$ 矛盾；所以 $p\nmid m$．现在 (5) 式给出 $g'(x)=0$，由此 $g(x)\in k[x^p]$；比如 $g(x)=g_2(x^p)$．因为 $x^{p^e}-c=g(x)^m$ 给出 $x^{p^{e-1}}-c=g_2(x)^m$，这是不可约多项式 $x^{p^{e-1}}-c$ 禁止的一个分解，由此迫使 $m=1$． ■

如果 E/k 是域扩张，其中 k 有特征 p，则 $k^p\subseteq E^p$，但我们不知道是否有 $k\subseteq E^p$；即 E^p 也许不是 E/k 的中间域（例如，取 $E=k$）．记添加 E^p 到 k 得到的 E 的子域为 $k(E^p)$．

命题 6.81 (i) 设 $k\subseteq B\subseteq E$ 是域塔且 E/k 是代数扩张．如果 E/k 是可分的，则 E/B 也是可分的．

(ii) 设 E/k 是代数域扩张，其中 k 有特征 $p>0$．如果 E/k 是可分扩张，则 $E=k(E^p)$．反之，如果 E/k 是有限的且 $E=k(E^p)$，则 E/k 是可分的．

证明 (i) 如果 $\alpha\in E$，则 α 是 B 上的代数元素，且在 $B[x]$ 中有 $\mathrm{irr}(\alpha,B)\mid\mathrm{irr}(\alpha,k)$，这是因为它们的 gcd 不是 1 且 $\mathrm{irr}(\alpha,B)$ 不可约．因 $\mathrm{irr}(\alpha,k)$ 无重根，$\mathrm{irr}(\alpha,B)$ 也无重根，因此 $\mathrm{irr}(\alpha,B)$ 是可分多项式．所以 E/B 是可分扩张．

(ii) 设 E/k 是可分扩张．现在 $k(E^p)\subseteq E$，从而根据 (i)，$E/k(E^p)$ 是可分扩张．但如果 $\beta\in E$，则 $\beta^p\in E^p\subseteq k(E^p)$；比如 $\beta^p=\alpha$．因此在 $(k(E^p))[x]$ 中有 $\mathrm{irr}(\beta,k(E^p))\mid(x^p-\alpha)$，因

$\mathrm{irr}(\beta,k(E^p))$ 整除 $x^p-\alpha=(x-\beta)^p$，所以它不是可分的．由此可知 $\beta\in k(E^p)$；即 $E=k(E^p)$．

反之，假设 $E=k(E^p)$．我们先证明：如果 $\beta_1,\cdots,\beta_s$ 是 E 中的线性无关表（其中 E 现在只看作 k 上的向量空间），则 $\beta_1^p,\cdots,\beta_s^p$ 也在 k 上线性无关．把 $\beta_1,\cdots,\beta_s$ 扩展为 E 的基 $\beta_1,\cdots,\beta_n$，其中 $n=[E:k]$．现在 $\beta_1^p,\cdots,\beta_n^p$ 在 k^p 上张成 E^p，这是因为如果 $\eta\in E$，则 $\eta=\sum_i a_i\beta_i$，其中 $a_i\in k$，因此 $\eta^p=\sum_i a_i^p\beta_i^p$．取任意元素 $\gamma\in E$，因 $E=k(E^p)$，有 $\gamma=\sum_j c_j\eta_j$，其中 $c_j\in k,\eta_j\in E^p$．但如同刚才我们已知的，存在 $a_{ji}\in k$ 使得 $\eta_j=\sum_i a_{ji}^p\beta_i^p$，从而 $\gamma=\sum_i\left(\sum_j c_j a_{ji}^p\right)\beta_i^p$，即 $\beta_1^p,\cdots,\beta_n^p$ 在 k 上张成 E．因 $\dim_k(E)=n$，所以这个表是基，因此它的子表 $\beta_1^p,\cdots,\beta_s^p$ 必在 k 上线性无关．

369

因 E/k 是有限的，每个 α 都是 k 上的代数元素．如果 $\mathrm{irr}(\alpha,k)$ 的次数为 m，则 $1,\alpha,\alpha^2,\cdots,\alpha^m$ 在 k 上线性相关，而 $1,\alpha,\alpha^2,\cdots,\alpha^{m-1}$ 线性无关．如果 α 是不可分的，则 $\mathrm{irr}(\alpha,k)=f_e(x^{p^e})$ 且 $m=p^e r$，其中 r 是 $\mathrm{irr}(\alpha,k)$ 的约化次数．因 $r=m/p^e<m$，所以有 $1,\alpha,\alpha^2,\cdots,\alpha^r$ 在 k 上线性无关．但 α^{p^e} 是 $f_e(x)$ 的根，从而在 $1,\alpha^{p^e},\alpha^{2p^e},\cdots,\alpha^{rp^e}$ 上存在非平凡的相关关系（因为 $rp^e=m$）．在前面一段我们已经看到，$1,\alpha,\alpha^2,\cdots,\alpha^r$ 线性无关蕴涵 $1,\alpha^{p^e},\alpha^{2p^e},\cdots,\alpha^{rp^e}$ 线性无关．这个矛盾表明 α 必是 k 上的可分元素． ■

系 6.82 *设 E/k 是有限可分扩张，其中 k 是特征 p 的域．如果 E 中的表 $\beta_1,\cdots,\beta_r$ 在 k 上线性无关，则对一切 $e\geqslant 1$，表 $\beta_1^{p^e},\cdots,\beta_r^{p^e}$ 在 k 上也线性无关．*

证明 对 $e\geqslant 1$ 用归纳法证明．和命题6.81(ii)的证明一样，在 $E=k(E^p)$ 中用可分性假设． ■

系 6.83 *如果 $k\subseteq B\subseteq E$ 是代数扩张塔，则 B/k 和 E/B 都是可分扩张当且仅当 E/k 是可分扩张．*

证明 因 B/k 和 E/B 是可分扩张，命题6.81(ii)给出 $B=k(B^p)$ 和 $E=B(E^p)$．因为 $B^p\subseteq E^p$，所以

$$E=B(E^p)=k(B^p)(E^p)=k(B^p\cup E^p)=k(E^p)\subseteq E,$$

由此，根据命题6.81(ii)，E/k 是可分的．

反之，如果 E 的每个元素在 k 上可分，则特别有 B 的每个元素在 k 上可分，因此 B/k 是可分扩张．最后，命题6.81(i)表明 E/B 是可分扩张． ■

命题 6.84 *如果 E/k 是代数扩张，定义*

$$E_s=\{\alpha\in E:\alpha\text{ 在 }k\text{ 上可分}\},$$

则 E_s 是一个中间域，它是 k 的包含在 E 中的唯一极大可分扩张．

证明 可由命题4.38(ii)得到，因为对 k 上可分的元素 α,β，$k(\alpha,\beta)/k$ 是可分的，因此 $\alpha+\beta,\alpha\beta$ 和 α^{-1} 在 k 上都是可分的． ■

不必惊奇，如果 E/k 是代数扩张，则扩张 E/E_s 具有特殊的性质．当然，只有当 k 有特征 $p>0$ 时 E_s 才是重要的（否则，$E_s=E$）．

下一类型的扩张是可分扩张的"补集"．

370

定义 *设 E/k 是域扩张，其中 k 有特征 $p>0$．则称 E/k 为***纯不可分扩张***，如果 E/k 是代数扩张，且对每个 $\alpha\in E$，存在 $e\geqslant 0$ 使得 $\alpha^{p^e}\in k$．*

如果 E/k 是纯不可分扩张且 B 是中间域，则 E/B 显然也是纯不可分的．

命题 6.85 如果 E/k 是代数域扩张，其中 k 有特征 $p>0$，则 E/E_s 是纯不可分扩张；此外，如果 $\alpha\in E$，则有某个 $m\geqslant 0$ 使得 $\operatorname{irr}(\alpha,E_s)=x^{p^m}-c$.

证明 如果 $\alpha\in E$，记 $\operatorname{irr}(\alpha,k)=f_e(x^{p^e})$，其中 $e\geqslant 0$ 和 $f_e(x)\in k[x]$ 是可分多项式．由此 α^{p^e} 在 k 上可分且 $\alpha^{p^e}\in E_s$．如果 $\alpha\notin E_s$，则选取极小的 m 使得 $\alpha^{p^m}\in E_s$．现在 α 是 $x^{p^m}-\alpha^{p^m}$ 的根，根据引理 6.80，这个多项式是不可约的，从而 $\operatorname{irr}(\alpha,E_s)=x^{p^m}-c$，其中 $c=\alpha^{p^m}$． ■

定义 如果 E/k 是有限扩张，则定义**可分次数**为 $[E:k]_s=[E_s:k]$，并定义**不可分次数**为 $[E:k]_i=[E:E_s]$.

注意 E/k 是可分的当且仅当 $[E:k]_i=1$．显然

$$[E:k]=[E:k]_s[E:k]_i.$$

命题 6.86 设 E/k 是有限扩张，其中 k 是特征 $p>0$ 的域．如果 E/k 是纯不可分的，则有某个 $e\geqslant 0$ 使得 $[E:k]=p^e$．因此对某个 $e\geqslant 0$ 有

$$[E:k]_i=[E:E_s]=p^e.$$

证明 如果 $\alpha\in E$，则 α 在 k 上是纯不可分的；如果 α 不是常数，则有某个 $c\in k$ 使得 $\operatorname{irr}(\alpha,E_s)=x^{p^m}-c$，其中 $m\geqslant 1$．所以，

$$[E:k]=[E:k(\alpha)][k(\alpha):k]=[E:k(\alpha)]p^m.$$

现在 $[E:k(\alpha)]<[E:k]$，因 $E/k(\alpha)$ 是纯不可分的，可以用归纳法完成证明．第二个陈述由命题 6.85 得到，因为 E 在 E_s 上是纯不可分的． ■

命题 6.87 如果 $k\subseteq B\subseteq E$ 是有限扩张的塔，其中 k 是特征 $p>0$ 的域，则

$$[E:k]_s=[E:B]_s[B:k]_s,\qquad [E:k]_i=[E:B]_i[B:k]_i.$$

371

证明 根据等式 $[E:k]=[E:k]_s[E:k]_i$，只要证明 $[E:k]_s=[E:B]_s[B:k]_s$．

记号 B_s 没有歧义，但这里的记号 E_s 有歧义．用 E_s 表示由 E 的在 k 上可分的一切元素组成的中间域，并记

$$E_B=\{\alpha\in E:\alpha\text{ 在 }B\text{ 上可分}\}.$$

我们有 $k\subseteq B_s\subseteq E_s\subseteq E_B\subseteq E$；接下来证明 $E_s\subseteq E_B$．如果 $\alpha\in E$ 在 k 上可分，则 $\operatorname{irr}(\alpha,k)$ 没有重根，因为在 $B[x]$ 中 $\operatorname{irr}(\alpha,B)\mid\operatorname{irr}(\alpha,k)$，所以 α 在 B 上可分，从而 $\alpha\in E_B$．使用这个记号，有

$$[E:k]_s=[E_s:k],[E:B]_s=[E_B:B]\text{ 和}[B:k]_s=[B_s:k].$$

现在

$$[E:k]_s=[E_s:k]=[E_s:B_s][B_s:k]=[E_s:B_s][B:k]_s.$$

因为 $[E_B:B]=[E:B]_s$，于是，只要证明

$$[E_s:B_s]=[E_B:B].$$

通过证明在 $E_s\subseteq E_B$ 中的表 $\beta_1,\cdots,\beta_r$ 在 B_s 上线性无关必在 B 上也线性无关，从而证明 $[E_s:B_s]\leqslant[E_B:B]$．假设 $\sum b_i\beta_i=0$，其中 $b_i\in B$ 不全为 0. 对一切 $e\geqslant 0$，我们有 $0=(\sum b_i\beta_i)^{p^e}=\sum b_i^{p^e}\beta_i^{p^e}$．但因为 B/B_s 是纯不可分的，所以存在 $e\geqslant 0$ 使得对一切 i，$b_i^{p^e}\in B_s$，从而表 $\beta_1^{p^e}\cdots,\beta_r^{p^e}$ 在 B_s 上线性无关，这和系 6.82 矛盾（因为 E_s/B_s 是可分扩张）．关于反过来的不等式 $[E_s:B_s]\geqslant[E_B:B]$，取 E_B 中在 B 上线性无关的表 $\gamma_1,\cdots,\gamma_t$．因 E_B/E_s 是纯不可分的（它是 E/E_s 的中间域），存在 $e\geqslant 0$ 使得对一切 i，$\gamma_i^{p^e}\in E_s$．但 E_s/B 是可分扩张，因此系 6.82 给出 $\gamma_1^{p^e}\cdots,\gamma_t^{p^e}$ 在 B 上线性

无关，因而 $\gamma_1^{p^e}\cdots,\gamma_t^{p^e}$ 在 B_s 上线性无关．所以 $[E_s:B_s]=[E_B:B]$. ■

关于可分性的更多结果我们仅作陈述．

定义　如果 A 和 B 都是域扩张 E/k 的中间域，则 A 和 B 称为**线性无缘**，如果 A 中的每个在 k 上线性无关的有限表 $\alpha_1,\cdots,\alpha_n$ 在 B 上线性无关．即如果 $\sum_i c_i\alpha_i=0$ 蕴涵只要一切 $c_i\in k$ 就有一切 $c_i=0$，则 $\sum_i\beta_i\alpha_i=0$ 蕴涵只要一切 $\beta_i\in B$ 就有一切 $\beta_i=0$.

可以证明在 A 和 B 上的这个条件是对称的；即 B 中的每个有限表在 k 上线性无关也在 A 上线性无关．在第 4 章中，我们定义了两个中间域 A 和 B 线性无缘如果 $A\cap B=k$．这个新的定义比老的更强：如果 $\alpha\in A$ 而 $\alpha\notin k$，则 $1,\alpha$ 在 k 上线性无关．如果 $\alpha\in A\cap B$，则 $-\alpha\cdot 1+1\cdot\alpha=0$ 是 B 上的一个相关关系（因为 $-\alpha,1\in B$）．然而，存在这样的例子，中间域 A 和 B 满足 $A\cap B=k$，但在这个新的意义下不是线性无缘的．

372

定义　设 k 是特征 p 的域，对 $n\geqslant 1$，定义

$$k^{1/p}=\{\alpha\in\bar{k}:\alpha^p\in k\},$$

其中 $\bar{k}$ 是 k 的代数闭包．

定理　一个代数域扩张 E/k 是可分的当且仅当 $k^{1/p}$ 和 E 是线性无缘的（作为 $\bar{E}/k$ 的中间域，其中 $\bar{E}$ 是 E 的代数闭包）．

证明　见 Zariski-Samuel 所著的《Commutative Algebra I》109 页． ■

如果不假定域扩张 E/k 是代数的，则命题6.81(ii)到 6.85 的结果仍然成立吗？

定义　域扩张 E/k 的一个**分离超越基**是指使得 $E/k(B)$ 成为可分扩张的超越基 B.

不是每个扩张 E/k 都有分离超越基．例如如果 E/k 是一个不可分代数扩张，则唯一的超越基是 $\varnothing$，但 $k(\varnothing)=k$ 且 $E/k(\varnothing)$ 是不可分的．

定理（麦克莱恩）　如果一个域扩张 E/k 有分离超越基，则 E 和 $k^{1/p}$ 是 $\bar{E}$ 的线性无缘的中间域，其中 $\bar{E}$ 是 E 的代数闭包．反之，如果 E 和 $k^{1/p}$ 是线性无缘的且 E/k 是有限生成的，即 $E=k\{u_1,\cdots,u_n\}$，则 E/k 有分离超越基．

证明　见 Jacobson 所著的《Basic Algebra II》，519 页． ■

下面的例子表明为什么在麦克莱恩（Mac Lane）定理中要假定 E/k 是有限生成的．

例 6.88　设 k 是特征 p 的完满域，$k(x)$ 是函数域，并定义

$$E=k(\{u_n,n\geqslant 1:u_n^{p^n}=x\}).$$

因 k 是完满的，k 的每个扩张都是可分的，从而 $E\cap k^{1/p}=k$．然而，我们断言 E/k 没有分离超越基．因为任一对 x^{1/p^n} 和 x^{1/p^m} 是代数相关的，根据习题 6.52，$\text{tr.deg}(E/k)=1$，设 $\{\beta\}$ 是超越基．现在 $k(\beta)\neq E$，从而存在某个 u_n 满足 $u_n\notin k(\beta)$，选取极小 n．考虑塔 $k(\beta)\subseteq k(\beta,u_n)\subseteq E$．如果 $\{\beta\}$ 是分离超越基，则根据命题 6.81(i)，$E/k(\beta,u_n)$ 是可分的．但因 $u_n\notin k(\beta)$，所以 $\text{irr}(u_n,k(\beta))$ 是 $y^{p^n}-x^{p^n}$ 的非线性因式，因此它有重根，所以 $E/k(\beta,u_n)$ 是不可分的，产生矛盾． ■

373

习题

6.41　设 k 是特征 $p>0$ 的域，并设 $f(x)=x^{2p}-x^p+t\in k(t)[x]$.

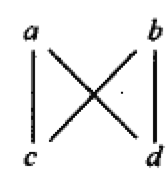
　(i) 证明 $f(x)$ 是 $k(t)[x]$ 中的不可约多项式．

（ⅱ）证明 $f(x)$ 是不可分的．

（ⅲ）证明存在代数扩张 $E/k(t)$，对于它没有中间域 E_i 能够使得 E_i/k 是纯不可分的且 E/E_i 是可分的．（比较系 6.85 和命题 4.38.）

6.42 设 m 是正整数，并设 X 是 m 的一切（正）因数的集合．如果定义 $a \preceq b$ 为 $a \mid b$，证明 X 是一个偏序集．

6.43 回忆如果 S 是偏序集 X 的子集，则 S 的**最小上界**(如果存在）是 S 的一个上界 m 使得对 S 的每个上界 u 有 $m \preceq u$．如果 X 是下面的偏序集（其中 $d \preceq a$ 是指 a 和 d 被一条线连接且 a 比 d 高），



证明子集 $S = \{c,d\}$ 有上界但没有最小上界．

6.44 设 G 是阿贝尔群，并设 $S \subseteq G$ 是子群．

（ⅰ）证明存在 G 的子群 H，它在具有性质 $H \cap S = \{0\}$ 的一切子群中极大．如果 G 不是阿贝尔群成立吗?

（ⅱ）如果 H 在满足 $H \cap S = \{0\}$ 的一切子群中极大，证明 $G/(H+S)$ 是挠群．

6.45 称偏序集 X 的子集 C 为**共尾的**，如果对每个 $x \in X$，存在 $c \in C$ 使得 $x \preceq c$．

（ⅰ）证明$\mathbb{Q}$ 和$\mathbb{Z}$ 都是$\mathbb{R}$ 的共尾子集．

（ⅱ）证明每个链 X 包含一个良序共尾子集．

提示：在 X 的一切良序子集的族上运用佐恩引理．

（ⅲ）证明 X 中的每个良序子集有上界当且仅当 X 中的每个链有上界．

6.46 （ⅰ）举出一个交换环的例子，它包含两个素理想 P 和 Q 但 $P \cap Q$ 不是素理想．

（ⅱ）如果 $P_1 \supseteq P_2 \supseteq \cdots P_n \supseteq P_{n+1} \cdots$ 是交换环 R 中素理想的降链，证明 $\bigcap_{n \geqslant 1} P_n$ 是素理想．

（ⅲ）证明每个交换环 R 有**极小素理想**，素理想 I 是**极小素理想**是指不存在素理想 P 满足 $P \subsetneq I$．

提示：在一切素理想的集合上用反包含作为偏序：$P \preceq Q$ 指 $P \supseteq Q$.

6.47 设 V 是向量空间，并设 S 是 V 的子空间．证明存在 V 的子空间 W，它在具有性质 $W \cap S = 0$ 和 $V = S \oplus W$ 的一切子空间中极大．

6.48 回忆交换环 R 的子集 S 称为**乘法封闭的**，如果 $0 \notin S$ 且 $s,s' \in S$ 蕴涵 $ss' \in S$．证明：如果 S 是乘法封闭的集合满足 $S \cap I = \varnothing$，则存在理想 J，满足 J 包含 I 且 $J \cap S = \varnothing$，并在具有这种性质的一切理想中极大，从而完成习题 6.9.

374

6.49 证明交换环中的任一非单位元素在某个极大理想之中．［这个结果用来解习题6.16(ⅱ).］

6.50 如果 $p_1,\cdots,p_n$ 是$\mathbb{Z}$ 中的不同素数，证明 $\sqrt{p_1},\cdots,\sqrt{p_n}$ 是$\mathbb{Q}$ 上的线性无关表．

6.51 证明域扩张 E/k 可能没有中间域 K 满足 K/k 是代数的且 E/K 是纯超越的．

提示：证明不存在中间域 K 满足$\mathbb{Q} \subseteq K \subsetneq \mathbb{C}$ 且$\mathbb{C}/K$ 是纯超越的．

6.52 如果 $E = k(X)$ 是域 k 的扩域，且每对 u，$v \in X$ 都是代数相关的，证明 $\mathrm{tr.deg}\,(E/k) \leqslant 1$．由此推出，如果

$$k \subseteq k_1 \subseteq k_2 \subseteq \cdots$$

是域塔，满足对一切 $n \geqslant 1$ 有 $\mathrm{tr.deg}\,(k_n/k) = 1$，则 $\mathrm{tr.deg}\,(k^*/k) = 1$，其中 $k^* = \bigcup_{n \geqslant 1} k_n$．

6.53 证明：如果 k 是域 E 的素域且 $\mathrm{tr.deg}\,(E/k) \leqslant \aleph_0$，则 E 是可数的．

6.54 证明两个特征相同的代数闭域同构当且仅当在它们的素域上有相同的超越次数．

提示：用引理 6.61.

6.55 （ⅰ）如果 $k \subseteq B \subseteq E$ 是域塔，证明

$$\mathrm{tr.deg}\,(E/k) = \mathrm{tr.deg}\,(E/B) + \mathrm{tr.deg}\,(B/k).$$

提示：证明如果 X 是 B/k 的超越基和 Y 是 E/B 的超越基，则 $X\cup Y$ 是 E/k 的超越基．

这个习题是错误的，给出一个反例。

（ⅱ）设 E/k 是域扩张，B 和 C 是中间域．证明

$$\text{tr.deg}\,(B\vee C)+\text{tr.deg}\,(B\cap C)=\text{tr.deg}\,(B)+\text{tr.deg}\,(C),$$

其中 $B\vee C$ 是复合域．

提示：把 $B\cap C$ 的一个超越基扩张成为 B 的超越基，并扩张成为 C 的超越基．

6.56 证明 $\varphi\in k(x)$ 的次数为 1 当且仅当 φ 是线性分式变换．

6.57 证明对每个域 k，$\mathrm{PGL}(2,k)\cong\mathrm{LF}(k)$，其中 $\mathrm{PGL}(2,k)=\mathrm{GL}(2,k)/Z(2,k)$，$Z(2,k)$ 是由一切（非零）标量矩阵组成的 $\mathrm{GL}(2,k)$ 的（正规）子群［$Z(2,k)$ 是 $\mathrm{GL}(2,k)$ 的中心］．

6.58 证明：如果 E/k 是代数扩张且 $\beta\in E$ 既是可分的又是纯不可分的，则 $\beta\in k$．

6.59 举出域扩张 E/k 的一个例子，它有两个中间域 A 和 B 满足 $A\cap B=k$，但 A 和 B 在 372 页定义的意义下不是线性无缘的．

375

6.5 簇

解析几何给出方程的图形．例如我们把函数：$f:\mathbb{R}\to\mathbb{R}$ 描画为它的图像，图像由平面上的一切有序对 $(a,f(a))$ 组成；即 f 是

$$g(x,y)=y-f(x)=0$$

的一切解 $(a,b)\in\mathbb{R}^2$ 的集合．我们也可以描画不是函数图像的那种方程．例如多项式

$$h(x,y)=x^2+y^2-1$$

的一切零点的集合是单位圆．我们还可以在 $\mathbb{R}^2$ 中画出几个二元多项式的共解，事实上，我们可以在 $\mathbb{R}^n$ 中画出几个 n 元多项式的共解．但在环 $k[x_1,\cdots,x_n]=k[X]$ 和 k^n 的子集的几何学之间存在的密切关系远远超过这一点．给定 n 元多项式 $f_1(X),\cdots,f_t(X)$ 的集合，它们的公共零点组成的子集 $V\subseteq k^n$ 称为簇．当然，我们可以研究簇，因为多项式方程组（线性方程组的明显推广）的解有它固有的重要性．另一方面，某些方程组会比另外一些更有趣，研究一个问题会导出一个簇，了解这个簇和它的性质（例如不可约性、维数、亏格、奇点等等）有助于了解原来的问题．例如，莱布尼茨提出函数的判定问题，即哪些函数的积分可以用“初等函数”表达出来，初等函数是指多项式、三角函数、反三角函数、指数函数和对数函数的代数组合．1694 年，约翰·伯努利（John Bernoulli）猜测由椭圆弧长产生的积分不能这样求出来．求摆的周期也产生类似的积分，还有力学中的其他问题，所有这些问题可以简化为形如

$$\int_0^x\frac{\mathrm{d}t}{\sqrt{p(t)}}$$

的积分，其中 $p(t)$ 是三次或四次多项式；即提出了 $\mathbb{R}[x,y]$ 中的多项式 $y^2-p(x)$．类似于

$$\sin^{-1}x=\int_0^x\frac{\mathrm{d}t}{\sqrt{1-t^2}},$$

雅可比引入反函数

$$u^{-1}(x)=\int_0^x\frac{\mathrm{d}t}{\sqrt{p(t)}},$$

376

他称 $u(x)$ 为椭圆函数．正如 $\sin x$ 经参数（$\sin x$，$\cos x$）确定单位圆，椭圆函数也经参数（$u(x)$，$u'(x)$）确定一条曲线，其中 $u'(x)$ 是 $u(x)$ 的导数．还注意到椭圆函数是周期的（和 $\sin x$ 一样）；即

存在某个数 q 使得对一切实数 x 和一切 $m \in \mathbb{Z}$, $u(x+mq)=u(x)$. 随着复变函数积分的发展，高斯把椭圆函数看作

$$u^{-1}(z)=\int_0^z \frac{\mathrm{d}w}{\sqrt{p(w)}},$$

其中 $p(w)$ 是 $\mathbb{C}(w)$ 中的三次或四次多项式；即提出了 $\mathbb{C}[z,u]$ 中的多项式 $u^2-p(z)$. 以这种方式看待椭圆函数，他知道它们是**双周期的**；即存在（复）数 q 和 r 使得对一切复数 z 和一切 $m,n \in \mathbb{Z}$ 有

$$u(z+mq+nr)=u(z).$$

此外，$u(z)$ 确定一条由一切 $(u(z),u'(z))$ 组成的复曲线（称为**椭圆曲线**）. 一维复空间是二维实空间，双周期说明这条复曲线是环面；即圆环面，可能有几个洞. 一个推论是椭圆函数的性状依赖于相伴的曲线是否是非奇异的；即它的每一点是否都有一个适当的切空间. 在黎曼把黎曼曲面引入椭圆函数和椭圆曲线研究的时候，该课题还远未完满. 但从此开创了一个十分丰富的课题[⊖]；确实，对这些问题更深入的研究本质上是在怀尔斯（A. Wiles）对费马最后定理的证明之中，他证明椭圆曲线具有某种成熟的性质. 更一般地说，$k[x_1,\cdots,x_n]$ 和簇之间的相互影响牵涉到今日所谓的代数几何，本节可以看作是这一课题的引言.

记号　设 k 是域，k^n 表示一切 n 元组的集合

$$k^n=\{a=(a_1,\cdots,a_n): 对一切\ i, a_i \in k\}.$$

多元多项式环 $k[x_1,\cdots,x_n]$ 可以记为 $k[X]$，其中 X 是缩写

$$X=(x_1,\cdots,x_n).$$

特别地，$f(x_1,\cdots,x_n) \in k[x_1,\cdots,x_n]$ 可以缩写为 $f(X) \in k[X]$.

下面，我们把多项式 $f(x_1,\cdots,x_n) \in k[x_1,\cdots,x_n]$ 看作 n 个变量 $k^n \to k$ 的函数，精确定义如下.

定义　如果 $f(X) \in k[X]$，定义它的**多项式函数** $f^\flat: k^n \to k$ 为赋值函数：如果 $(a_1,\cdots,a_n) \in k^n$，则

$$f^\flat: (a_1,\cdots,a_n) \mapsto f(a_1,\cdots,a_n).$$

377　下一命题把系 3.28 从单变量推广到多变量.

命题 6.89　设 k 是一个无限域，并设 $k[X]=k[x_1,\cdots,x_n]$. 如果 $f(X),g(X) \in k[X]$ 满足 $f^\flat=g^\flat$，则 $f(x_1,\cdots,x_n)=g(x_1,\cdots,x_n)$.

证明　对 $n \geqslant 1$ 用归纳法证明. 基础步是系 3.28. 关于归纳步，记

$$f(X,y)=\sum_i p_i(X)y^i \text{ 和 } g(X,y)=\sum_i q_i(X)y^i,$$

其中 X 表示 $(x_1,\cdots,x_n)$. 如果 $f^\flat=g^\flat$，则对每个 $a \in k^n$ 和每个 $\beta \in k$ 有 $f(a,\beta)=g(a,\beta)$. 对固定的 $a \in k^n$，定义 $F_a(y)=\sum_i p_i(a)y^i$ 和 $G_a(y)=\sum_i q_i(a)y^i$. 因 $F_a(y)$ 和 $G_a(y)$ 两者都在 $k[y]$ 中，基础步给出对一切 $a \in k^n$，$p_i(a)=q_i(a)$. 由归纳假设，对一切 i，$p_i(X)=q_i(X)$，因此正如所要的，

$$f(X,y)=\sum_i p_i(X)y^i=\sum_i q_i(X)y^i=g(X,y).$$ ■

基于上面的命题，当 k 无限时，我们放弃记号 $f^\flat$，而把多项式和它们的多项式函数等同起来.

定义　如果 $f(X) \in k[X]=k[x_1,\cdots,x_n]$，$f(a)=0$，其中 $a \in k^n$，则 a 称为 $f(X)$ 的一个**零点**. [如果 $f(x)$ 是一元多项式，则 $f(x)$ 的零点也称为 $f(x)$ 的根.]

命题 6.90　如果 k 是代数闭域且 $f(X) \in k[X]$ 不是常数，则 $f(X)$ 有零点.

⊖　要从容地、详细地了解椭圆函数的发展，见 Stillwell 所著的《Mathematics and Its History》第 14 和 15 章.

证明 对 $n \geqslant 1$ 用归纳法证明，其中 $X = (x_1, \cdots, x_n)$．基础步可以从假设 $k^1 = k$ 是代数闭的立刻得到．和前面的证明一样，记

$$f(X,y) = \sum_i g_i(X) y^i.$$

对每个 $a \in k^n$ 定义 $f_a(y) = \sum_i g_i(a) y^i$．如果 $f(X,y)$ 没有零点，则每个 $f_a(y) \in k[y]$ 都没有零点，于是基础步说对一切 $a \in k^n$，$f_a(y)$ 都是一个非零常数．由此，对一切 $i > 0$ 和一切 $a \in k^n$，$g_i(a) = 0$．因代数闭域是无限的，运用命题 6.89，对一切 $i > 0$ 有 $g_i(X) = 0$，从而 $f(X,y) = g_0(X) y^0 = g_0(X)$．由归纳假设，$g_0(x)$ 是非零常数，证明完成． ■

378

我们现在给出描述多项式的解集的几个一般定义．

定义 如果 F 是 $k[X] = k[x_1, \cdots, x_n]$ 的子集，则由 F 定义的**簇**[⊖][⊜]是

$$\mathrm{Var}(F) = \{a \in k^n : 对每个\ f(X) \in F, f(a) = 0\}.$$

这样，$\mathrm{Var}(F)$ 由那些成为每个 $f(X) \in F$ 零点的一切 $a \in k^n$ 组成．

例 6.91 （i）如果 k 是代数闭的，则命题 6.90 说如果 $f(X) \in k[X]$ 不是常数，则 $\mathrm{Var}(f(X)) \neq \varnothing$．

（ii）这里是由两个方程定义的几个簇：

$$\mathrm{Var}(x,y) = \{(a,b) \in k^2 : x = 0, y = 0\} = \{(0,0)\}$$

和

$$\mathrm{Var}(xy) = x\text{-轴} \cup y\text{-轴}.$$

（iii）这里是高维空间的一例．设 A 是元素在 k 中的 $m \times n$ 矩阵．n 个未知数 m 个方程的方程组

$$AX = B,$$

其中 B 是 $n \times 1$ 列矩阵，定义了一个簇，$\mathrm{Var}(AX = B)$，它是 k^n 的子集．当然 $AX = B$ 其实就是 n 个变量 m 个线性方程的集合的缩写，常称 $\mathrm{Var}(AX = B)$ 为方程组 $AX = B$ 的**解集**．当这个方程组是齐次的时候，即 $B = 0$ 时，$\mathrm{Var}(AX = 0)$ 是 k^n 的子空间，称为方程组的**解空间**． ■

下面的结果表明只要涉及簇，就可以假定 $k[X]$ 的子集 F 是 $k[X]$ 的理想．

379

命题 6.92 设 k 是域，并设 F 和 G 是 $k[X]$ 的子集．

⊖ 关于这个术语的用法有几个不同的意见．有些人称它为仿射簇，和射影簇相对照．有些人强调簇应该是不可约的，对此我们将在本节的后面定义．

⊜ 术语 variety（簇）产生自 E. Beltrami 翻译的德语术语 Mannigfaltigkeit（高斯授意的），该术语由黎曼使用，现在该术语常翻译为 manifold（流形）．下面的 Aldo Brigaglia 给 Steven Kleiman 的信件包含更详细的内容．

"我相信意大利几何学者使用的字 varietà 来自黎曼的 Habilitationsvortrag（未发表）的意大利语翻译，后来 J. Hoüel 把它翻译为法语并发表在意大利期刊 Annali 上．确实，1869 年 1 月 8 日 Beltrami 写给 Hoüel 道：

J'ai traduit Mannigfaltigkeit par varietà, dans le sens de multitudo variarum rerum...

后来，1869 年 2 月 14 日他写道：

Je croirais toujours convenable de traduire Mannigfaltigkeit par variété: j'ai remarqué que Gauss, dans ses Mémoires sur les résidus biquadratiques appelle en latin varietas la même chose qui, dans les comptes-rendus rédigés par lui même en allemand dans les Gelehrte Anzeige, est désignée par Mannigfaltigkeit.

Beltrami 和 Hoüel 的通信可以在一本好书《La découverte de la géométrie non euclidienne sur la pseudosphère: les lettres d'Eugenio Beltrami à Jules Hoüel (1868—1881)》中找到，L. Boi，L. Giacardi 和 R. Tazzioli 编辑，Blanchard 出版，巴黎，1998."

（i）如果 $F \subseteq G \subseteq k[X]$，则 $\mathrm{Var}(G) \subseteq \mathrm{Var}(F)$．

（ii）如果 $F \subseteq k[X]$ 且 $I = (F)$ 是 F 生成的理想，则

$$\mathrm{Var}(F) = \mathrm{Var}(I).$$

证明 （i）如果 $a \in \mathrm{Var}(G)$，则对一切 $g(X) \in G$，$g(a) = 0$．因 $F \subseteq G$，从而特别对一切 $f(X) \in F$ 有 $f(a) = 0$．

（ii）因 $F \subseteq (F) = I$，根据（i），$\mathrm{Var}(I) \subseteq \mathrm{Var}(F)$．关于反包含，设 $a \in \mathrm{Var}(F)$，从而对每个 $f(X) \in F$ 有 $f(a) = 0$．如果 $g(X) \in I$，则 $g(X) = \sum_i r_i(X) f_i(X)$，其中 $r_i(X) \in k[X]$，$f_i(X) \in F$；因此 $g(a) = \sum_i r_i(a) f_i(a) = 0$，从而 $a \in \mathrm{Var}(I)$． ■

由此，并非 k^n 的每个子集都是簇．例如，如果 $n = 1$，则 $k[x]$ 是 PID. 因此，如果 F 是 $k[x]$ 的子集，则有某个 $g(x) \in k[x]$ 使得 $(F) = (g(x))$，从而

$$\mathrm{Var}(F) = \mathrm{Var}((F)) = \mathrm{Var}((g(x))) = \mathrm{Var}(g(x)).$$

但如果 $g(x) \neq 0$，则 $g(x)$ 的根是有限的，从而 $\mathrm{Var}(F)$ 有限．如果 k 是代数闭的，它必是无限域，因此 $k^1 = k$ 的多数子集不是簇．

尽管我们希望在平面上作图，但是 $k = \mathbb{R}$ 时有一个主要的缺点：某些多项式无零点．例如，$f(x) = x^2 + 1$ 无实根，因此 $\mathrm{Var}(x^2 + 1) = \varnothing$．更一般地，$g(x_1, \cdots, x_n) = x_1^2 + \cdots + x_n^2 + 1$ 在$\mathbb{R}^n$ 中无零点，因此 $\mathrm{Var}(g(X)) = \varnothing$．因我们所处理的是（不必线性）多项式，自然假定它们的零点都是可以得到的．对于一元多项式，意味着 k 是代数闭的，根据命题 6.90 我们知道，如果 k 是代数闭的，则对每个非常数的 $f(X) \in k[X]$，$\mathrm{Var}(f(X)) \neq \varnothing$．当然，簇对于一切域 k 都是重要的，但在试图理解更复杂的问题之前，先考虑最简单的情形更容易明白．另一方面，许多初始结果适用于任意域．这样，我们会对每个命题说明必需的假设，但读者要明白最重要的情形是 k 为代数闭域．

下面是簇的一些初等性质．

命题 6.93 设 k 是域．

（i）$\mathrm{Var}(1) = \varnothing$，$\mathrm{Var}(0) = k^n$，其中 0 是零多项式．

（ii）如果 I 和 J 是 $k[X]$ 中的理想，则

$$\mathrm{Var}(IJ) = \mathrm{Var}(I \cap J) = \mathrm{Var}(I) \cup \mathrm{Var}(J),$$

380

其中 $IJ = \left\{ \sum_i f_i(X) g_i(X) : f_i(X) \in I, g_i(X) \in J \right\}$.

（iii）如果 $\{I_\ell : \ell \in L\}$ 是 $k[X]$ 中理想的族，则

$$\mathrm{Var}\left(\sum_\ell I_\ell\right) = \bigcap_\ell \mathrm{Var}(I_\ell),$$

其中 $\sum_\ell I_\ell$ 是形如 $r_{\ell_1} + \cdots + r_{\ell_q}$ 的一切有限和的集合，其中 $r_{\ell_i} \in I_{\ell_i}$．

证明 （i）因为常数多项式 1 没有根，显然 $\mathrm{Var}(1) = \varnothing$．因为每个点 a 都是零多项式的零点，所以 $\mathrm{Var}(0) = k^n$．

（ii）因 $IJ \subseteq I \cap J$，所以有 $\mathrm{Var}(IJ) \supseteq \mathrm{Var}(I \cap J)$；因 $IJ \subseteq I$，所以有 $\mathrm{Var}(IJ) \supseteq \mathrm{Var}(I)$. 由此，

$$\mathrm{Var}(IJ) \supseteq \mathrm{Var}(I \cap J) \supseteq \mathrm{Var}(I) \cup \mathrm{Var}(J).$$

要完成证明，只需证明 $\mathrm{Var}(IJ) \subseteq \mathrm{Var}(I) \cup \mathrm{Var}(J)$．如果 $a \notin \mathrm{Var}(I) \cup \mathrm{Var}(J)$，则存在 $f(X) \in I$ 和 $g(X) \in J$ 使得 $f(a) \neq 0$ 且 $g(a) \neq 0$．但因 k 是整环，有 $f(X)g(X) \in IJ$ 和 $(fg)(a) =$

$f(a)g(a)\neq 0$. 所以，正如所要的 $a\notin \mathrm{Var}(IJ)$.

（iii）对每个 ℓ，包含关系 $I_\ell\subseteq\sum_\ell I_\ell$ 给出 $\mathrm{Var}\left(\sum_\ell I_\ell\right)\subseteq \mathrm{Var}(I_\ell)$，从而

$$\mathrm{Var}\left(\sum_\ell I_\ell\right)\subseteq\bigcap_\ell \mathrm{Var}(I_\ell).$$

关于反包含，如果 $g(X)\in\sum_\ell I_\ell$，则存在有限个 ℓ 使得 $g(X)=\sum_\ell f_\ell$，其中 $f_\ell(X)\in I_\ell$. 因此，如果 $a\in\bigcap_\ell \mathrm{Var}(I_\ell)$，则对一切 ℓ，$f_\ell(a)=0$，从而 $g(a)=0$；即 $a\in \mathrm{Var}\left(\sum_\ell I_\ell\right)$. ■

定义　拓扑空间是指集合 X 连同 X 的一个称为**闭集**[⊖]的子集族 $\mathcal{F}$，它满足下列公理：

（i）$\varnothing\in\mathcal{F}$ 和 $X\in\mathcal{F}$；

（ii）如果 $F_1,F_2\in\mathcal{F}$，则 $F_1\cup F_2\in\mathcal{F}$；即两个闭集的并也是闭集；

（iii）如果 $\{F_\ell:\ell\in L\}\subseteq\mathcal{F}$，则 $\bigcap_\ell F_\ell\in\mathcal{F}$；即闭集的任意交集也是闭集.

命题 6.93 证明一切簇的族是使得 k^n 成为一个拓扑空间的闭集. 称簇为**扎里斯基闭集**，它在深入研究 $k[X]$ 时十分有用. 通常有多种闭集可以把 $\mathbb{R}$ 看作拓扑空间，例如，每个闭区间是一个闭集. 与此相反，除了 $\mathbb{R}$ 自身之外 $\mathbb{R}$ 中只有有限集才是扎里斯基闭集.

定义　k^n 中的一个**超曲面**是形如 $\mathrm{Var}(f)$ 的子集，其中 f 是某个非常数多项式 $f(X)\in k[X]$.　381

系 6.94　k^n 中的每个簇 $\mathrm{Var}(I)$ 都是有限个超曲面的交.

证明　由希尔伯特基定理，存在 $f_1(X),\cdots,f_t(X)\in k[X]$ 使得 $I=(f_1,\cdots,f_t)=\sum_i(f_i)$. 根据命题6.93(iii)，有 $\mathrm{Var}(I)=\bigcap_i \mathrm{Var}(f_i)$. ■

给定 $k[X]$ 中的一个理想 I，我们已经定义了它的簇 $\mathrm{Var}(I)\subseteq k^n$. 现在反过来：给定一个子集 $A\subseteq k^n$，我们对它设计 $k[X]$ 中的一个理想，特别地，对每个簇设计一个理想.

定义　如果 $A\subseteq k^n$，定义它的**坐标环** $k[A]$ 为点态运算之下的交换环

$$k[A]=\{f^\flat\mid A: f(X)\in k[X]\}$$

[回忆 $f^\flat: k^n\to k$ 是由 $f(X)$ 形成的多项式函数].

当把多项式 $f(x_1,\cdots,x_n)=x_i\in k[X]$ 看作多项式函数时，它的定义是

$$x_i:(a_1,\cdots,a_n)\mapsto a_i;$$

即 x_i 挑出 k^n 中的一个点的第 i 个坐标. 叫做坐标环的理由是：如果 $a\in V$，则 $(x_1(a),\cdots,x_n(a))$ 描述了 a.

有一个明显的环同态 $\mathrm{res}: k[X]\to k[A]$，它由 $f(X)\mapsto f^\flat\mid A$ 给出，这个限制映射的核是 $k[X]$ 中的一个理想. 从现在起，我们假定所有的域 k 都是无限的，从而不再使用记号 $f^\flat$.

定义　如果 $A\subseteq k^n$，定义

$$\mathrm{Id}(A)=\{f(X)\in k[X]=k[x_1,\cdots,x_n]:\text{对每个 } a\in A \text{ 有 } f(a)=0\}.$$

希尔伯特基定理告诉我们 $\mathrm{Id}(A)$ 恒为有限生成理想.

命题 6.95　如果 $A\subseteq k^n$，则存在同构

$$k[X]/\mathrm{Id}(A)\cong k[A],$$

其中 $k[A]$ 是 A 的坐标环.

⊖ 我们也可以用指定开集来定义拓扑空间，开集定义为闭集的补集.

证明 限制映射 res: $k[X]\to k[A]$ 是满射，核为 $\mathrm{Id}(A)$，从而由第一同构定理可得结果．注意，在 A 上一致的两个多项式位于 $\mathrm{Id}(A)$ 的同一陪集之中． ■

虽然 $\mathrm{Var}(F)$ 的定义对 $k[X]$ 的任意子集 F 都有意义，但最重要的是 F 为理想．同样，尽管 $\mathrm{Id}(A)$ 的定义对 k^n 的任意子集 A 都有意义，但最重要的是 A 为簇．毕竟簇是由（多项式）方程的解组成的，而这是我们所关心的．

382

命题 6.96 设 k 是域．

（i）$\mathrm{Id}(\varnothing)=k[X]$，如果 k 是无限的，则 $\mathrm{Id}(k^n)=\{0\}$．

（ii）如果 $A\subseteq B$ 是 k^n 的子集，则 $\mathrm{Id}(B)\subseteq \mathrm{Id}(A)$．

（iii）如果 $\{A_\ell:\ell\in L\}$ 是 k^n 的子集族，则

$$\mathrm{Id}\Big(\bigcup_\ell A_\ell\Big)=\bigcap_\ell \mathrm{Id}(A_\ell).$$

证明 （i）由定义，对某个子集 $A\subseteq k^n$ 有 $f(X)\in\mathrm{Id}(A)$ 当且仅当对一切 $a\in A$ 有 $f(a)=0$；因此，如果 $f(X)\notin\mathrm{Id}(A)$，则存在 $a\in A$ 使得 $f(a)\neq 0$．特别地，如果 $A=\varnothing$，则没有元素 $a\in\varnothing$，从而每个 $f(X)\in k[X]$ 必在 $\mathrm{Id}(\varnothing)$ 中．所以 $\mathrm{Id}(\varnothing)=k[X]$．

如果 $f(X)\in\mathrm{Id}(k^n)$，则 $f^\flat=0^\flat$，因 k 是无限的，根据命题 6.89，$f(X)=0$．

（ii）如果 $f(X)\in\mathrm{Id}(B)$，则对一切 $b\in B$，$f(b)=0$；特别地，因 $A\subseteq B$，对一切 $a\in A$ 有 $f(a)=0$，从而 $f(X)\in\mathrm{Id}(A)$．

（iii）对一切 ℓ，因 $A_\ell\subseteq\bigcup_\ell A_\ell$，所以有 $\mathrm{Id}(A_\ell)\supseteq\mathrm{Id}\Big(\bigcup_\ell A_\ell\Big)$；因此 $\bigcap_\ell \mathrm{Id}(A_\ell)\supseteq\mathrm{Id}\Big(\bigcup_\ell A_\ell\Big)$．关于反包含，假设 $f(X)\in\bigcap_\ell\mathrm{Id}(A_\ell)$，即对一切 ℓ 和一切 $a_\ell\in A_\ell$，$f(a_\ell)=0$．如果 $b\in\bigcup_\ell A_\ell$，则有某个 ℓ 使得 $b\in A_\ell$，因此 $f(b)=0$；所以 $f(X)\in\mathrm{Id}\Big(\bigcup_\ell A_\ell\Big)$． ■

对于 $\mathrm{Id}(A\cap B)$ 我们希望有一个公式．当然，$\mathrm{Id}(A\cap B)=\mathrm{Id}(A)\cup\mathrm{Id}(B)$ 不成立，因为两个理想的并几乎不可能再成为理想．

为了刻画当 V 是簇时形如 $\mathrm{Id}(V)$ 的理想，产生了下面的思想．

定义 设 I 是交换环 R 的理想，则它的**根**（记为$\sqrt{I}$）是指

$$\sqrt{I}=\{r\in R:\text{有某个整数 } m\geqslant 1 \text{ 使得 } r^m\in I\}.$$

理想 I 称为**根理想**[⊖]，如果

$$\sqrt{I}=I.$$

习题 6.62 要求证明$\sqrt{I}$是理想．易知 $I\subseteq\sqrt{I}$，由此一个理想 I 是根理想当且仅当$\sqrt{I}\subseteq I$．例如，每个素理想 P 都是根理想，这是因为如果 $f^n\in P$ 则 $f\in P$．这里有一个不是根理想的理想的例子．设 $b\in k$ 和 $I=((x-b)^2)$，因为 $(x-b)^2\in I$ 而 $x-b\notin I$，所以 I 不是根理想．

定义 交换环 R 中的元素 a 称为**幂零的**，如果 $a\neq 0$ 且存在 $n\geqslant 1$ 使得 $a^n=0$．

注意，I 是交换环 R 中的根理想当且仅当 R/I 没有非零的幂零元素．没有幂零元素的交换环叫做**约化环**．

383

命题 6.97 如果对某个 $A\subseteq k^n$，理想 $I=\mathrm{Id}(A)$，则 I 是一个根理想．因此，坐标环 $k[A]$ 没有非零的幂零元素．

⊖ 这个术语是恰当的，因为当 $r^m\in I$ 时，它的 m 次根 r 也在 I 中．

证明 因恒有 $I\subseteq\sqrt{I}$，所以只要证明反包含．由假设，存在某个 $A\subseteq k^n$ 使得 $I=\mathrm{Id}(A)$；因此，如果 $f\in\sqrt{I}$，则 $f^m\in\mathrm{Id}(A)$；即对一切 $a\in A$，$f(a)^m=0$．但 $f(a)^m$ 的值在域 k 中，因此 $f(a)^m=0$ 蕴涵 $f(a)=0$；即 $f\in\mathrm{Id}(A)=I$． ■

命题 6.98 （i）如果 I 和 J 都是理想，则 $\sqrt{I\cap J}=\sqrt{I}\cap\sqrt{J}$．

（ii）如果 I 和 J 都是根理想，则 $I\cap J$ 也是根理想．

证明 （i）如果 $f\in\sqrt{I\cap J}$，则有某个 $m\geqslant1$ 使得 $f^m\in I\cap J$．因此 $f^m\in I$ 和 $f^m\in J$，从而 $f\in\sqrt{I}$ 和 $f\in\sqrt{J}$，即 $f\in\sqrt{I}\cap\sqrt{J}$．

关于反包含，假定 $f\in\sqrt{I}\cap\sqrt{J}$，于是 $f^m\in I$ 和 $f^q\in J$．我们可以假定 $m\geqslant q$，从而 $f^m\in I\cap J$，即 $f\in\sqrt{I\cap J}$．

（ii）如果 I 和 J 都是根理想，则 $I=\sqrt{I}$ 和 $J=\sqrt{J}$，且

$$I\cap J\subseteq\sqrt{I\cap J}=\sqrt{I}\cap\sqrt{J}=I\cap J.$$ ■

现在对$\mathbb{C}[X]$证明希尔伯特零点定理．读者将看到我们给出的证明可以推广到任意不可数代数闭域．事实上该定理对一切代数闭域都成立（我们将在第 11 章给出证明），然而这里的证明不能涵盖素域的代数闭包，例如，它可能是可数的．

引理 6.99 设 k 是域且 $\varphi: k[X]\to k$ 是逐点固定 k 的满射环同态．如果 $J=\ker\varphi$，则 $\mathrm{Var}(J)\neq\varnothing$．

证明 设 $\varphi(x_i)=a_i\in k$ 并设 $a=(a_1,\cdots,a_n)\in k^n$．如果

$$f(X)=\sum_{\alpha_1,\cdots,\alpha_n}c_{\alpha_1,\cdots,\alpha_n}x_1^{\alpha_1}\cdots x_n^{\alpha_n}\in k[X],$$

则

$$\begin{aligned}\varphi(f(X))&=\sum_{\alpha_1,\cdots,\alpha_n}c_{\alpha_1,\cdots,\alpha_n}\varphi(x_1)^{\alpha_1}\cdots\varphi(x_n)^{\alpha_n}\\&=\sum_{\alpha_1,\cdots,\alpha_n}c_{\alpha_1,\cdots,\alpha_n}a_1^{\alpha_1}\cdots a_n^{\alpha_n}\\&=f(a_1,\cdots,a_n)\\&=f(a).\end{aligned}$$

因此，如果 $f(X)\in J=\ker\varphi$，则 $f(a)=0$，从而 $a\in\mathrm{Var}(J)$． ■

384

下一个证明要用到一点基数．

定理 6.100（$\mathbb{C}$上的弱零点定理[⊖]） 如果 $f_1(X),\cdots,f_t(X)\in\mathbb{C}[X]$，则 $I=(f_1,\cdots,f_t)$ 是$\mathbb{C}[X]$中的真理想当且仅当 $\mathrm{Var}(f_1,\cdots,f_t)\neq\varnothing$．

注 读者需注意，证明中关于$\mathbb{C}$的性质只用到$\mathbb{C}$是不可数代数闭域．

证明 显然，如果 $\mathrm{Var}(I)\neq\varnothing$，则因 $\mathrm{Var}(\mathbb{C}[X])=\varnothing$，所以 I 是真理想．

反之，假定 I 是真理想．根据系 6.40，存在极大理想 M 包含 I，从而 $K=\mathbb{C}[X]/M$ 是域．显然，自然映射$\mathbb{C}[X]\to\mathbb{C}[X]/M=K$ 把$\mathbb{C}$带到它自己，从而 $K/\mathbb{C}$ 是域扩张，由此 K 是$\mathbb{C}$上的向量空间．现在$\mathbb{C}[X]$作为$\mathbb{C}$-空间，对由一切首一单项式 $1,x,x^2,x^3,\cdots$ 组成的一个基有可数维数．因为 K 是$\mathbb{C}[X]$的商，所以 $\dim_{\mathbb{C}}(K)$ 是可数的（可能有限），

⊖ 德语字 Nullstelle 的意思是根．在多元多项式的上下文中，我们可以把它翻译为零点，从而 Nullstellensatz 的意思是零点定理．

假设 K 是$\mathbb{C}$的真扩张，即存在某个 $t \in K$ 满足 $t \notin \mathbb{C}$. 因$\mathbb{C}$是代数闭的，t 不可能是$\mathbb{C}$上的代数元素，从而它是超越的．考虑 K 的子集 B，

$$B = \{1/(t-c) : c \in \mathbb{C}\}$$

（注意，因为 $t \notin \mathbb{C}$，所以 $t-c \neq 0$）．集合 B 由不可数集合$\mathbb{C}$加标，所以它是不可数的．我们断言 B 在$\mathbb{C}$上线性无关，如果确实如此，则与 $\dim_{\mathbb{C}}(K)$ 是可数的矛盾，由此可知 $K=\mathbb{C}$. 如果 B 线性相关，则存在非零的 $a_1,\cdots,a_r \in \mathbb{C}$ 和不同的 $c_1,\cdots,c_r \in \mathbb{C}$ 使得 $\sum_{i=1}^{r} a_i/(t-c_i) = 0$．通分得多项式 $h(t) \in \mathbb{C}[t]$：

$$h(t) = \sum_i a_i(t-c_1)\cdots\widehat{(t-c_i)}\cdots(t-c_r) = 0.$$

现在 $h(c_1) = a_1(c_1-c_2)\cdots(c_1-c_r) \neq 0$，从而 $h(t)$ 不是零多项式．但这与 t 是超越元素矛盾．所以 $K=\mathbb{C}$. 现在运用引理 6.99 表明 $\mathrm{Var}(M) \neq \varnothing$．但 $\mathrm{Var}(M) \subseteq \mathrm{Var}(I)$，证明完成． ■

考虑这个定理对于 $I = (f(x)) \subseteq \mathbb{C}[x]$ 的特殊情形，其中 $f(x)$ 不是常数．说 $\mathrm{Var}(f) \subseteq \mathbb{C}$ 非空，也就是说 $f(x)$ 有复根．由此，弱零点定理把代数基本定理推广到多元的情形．

下面希尔伯特零点定理的证明运用了"Rabinowitch 技巧"，把一个 n 元多项式环嵌入到一个 $n+1$ 元多项式环．不可数性依然不是必需的，我们作此假定仅仅因为对弱零点定理的证明使用了这个假设．

定理 6.101（零点定理） 设 k 是（不可数）代数闭域．如果 I 是 $k[X]$ 中的理想，则 $\mathrm{Id}(\mathrm{Var}(I)) = \sqrt{I}$．于是，$f$ 在 $\mathrm{Var}(I)$ 上成为零当且仅当有某个 $m \geqslant 1$ 使得 $f^m \in I$.

证明 如果对某个 $m \geqslant 1$ 和一切 $a \in \mathrm{Var}(I)$ 有 $f^m(a) = 0$，则因 $f(a) \in k$，所以对一切 a 有 $f(a)=0$，由此包含关系 $\mathrm{Id}(\mathrm{Var}(I)) \supseteq \sqrt{I}$ 显然成立．

反之，假定 $h \in \mathrm{Id}(\mathrm{Var}(I))$，其中 $I=(f_1,\cdots,f_t)$；即如果对一切 i 有 $f_i(a)=0$，其中 $a \in k^n$，则 $h(a)=0$．我们需要证明 h 的某个幂在 I 中．当然，可以假定 h 不是零多项式．可以认为

$$k[x_1,\cdots x_n] \subseteq k[x_1,\cdots,x_n,y];$$

于是，把每个 $f_i(x_1,\cdots,x_n)$ 看作不依赖于最后一个变量 y 的 $n+1$ 元多项式．我们断言多项式

$$f_1,\cdots,f_t,1-yh$$

在 $k[x_1,\cdots,x_n,y]$ 中没有公共零点．如果 $(a_1,\cdots,a_n,b) \in k^{n+1}$ 是公共零点，则 $a=(a_1,\cdots,a_n) \in k^n$ 是 $f_1,\cdots,f_t$ 的公共零点，从而 $h(a)=0$．但 $1-bh(a)=1\neq 0$．现在运用弱零点定理表明 $k[x_1,\cdots,x_n,y]$ 中的理想 $(f_1,\cdots,f_t,1-yh)$ 不是真理想．所以存在 $g_1,\cdots,g_{t+1} \in k[x_1,\cdots,x_n,y]$ 使得

$$1 = f_1g_1+\cdots+f_tg_t+(1-yh)g_{t+1}.$$

作替换 $y=1/h$，于是含有 g_{t+1} 的最后一项消失．重写得 $g_i(X,y)=\sum_{j=0}^{d_i} u_j(X)y^j$，从而 $g_i(X,h^{-1}) = \sum_{j=0}^{d_i} u_j(X)h^{-j}$．由此

$$h^{d_i}g_i(X,h^{-1}) \in k[X].$$

所以，如果 $m=\max\{d_1,\cdots,d_t\}$，则

$$h^m = (h^mg_1)f_1+\cdots+(h^mg_t)f_t \in I.$$ ■

定理 6.102 如果 k 是一个（不可数的）代数闭域，则 $k[x_1,\cdots,x_n]$ 中的每个极大理想 M 形如

$$M=(x_1-a_1,\cdots,x_n-a_n),$$

其中 $a=(a_1,\cdots,a_n)\in k^n$，从而存在 k^n 和 $k[x_1,\cdots,x_n]$ 中的极大理想之间的双射.

注 不可数性的假设将在第 11 章中去掉.

证明 根据定理 6.101，$\mathrm{Id}(\mathrm{Var}(M))=\sqrt{M}=M$，因为 M 是极大的，因而是素理想. 由于 M 是真理想，根据定理 6.100 有 $\mathrm{Var}(M)\neq\varnothing$；也就是说，存在 $a=(a_1,\cdots,a_n)\in k^n$，对一切 $f\in M$ 有 $f(a)=0$. 于是，$\{a\}\subseteq\mathrm{Var}(M)=\{b\in k^n: f(b)=0$，对所有 $f\in M\}$，命题 6.92 给出 $M=\mathrm{Id}(\mathrm{Var}(M))\subseteq\mathrm{Id}(\{a\})$. 因 $\mathrm{Id}(\{a\})$ 不包含任何非零常数，故它是真理想，且 M 的极大性给出 $M=\mathrm{Id}(\{a\})=\{f(X)\in k[X]: f(a)=0\}$. 对每个 i，定义 $f_i(X)=x_i-a_i$. 现在 $f_i(a)=0$，因此 $(f_1,\cdots,f_n)\subseteq\mathrm{Id}(\{a\})$. 但根据习题 6.6(i)，$(x_1-a_1,\cdots,x_n-a_n)$ 是极大理想，从而 $(f_1,\cdots,f_n)=(x_1-a_1,\cdots,x_n-a_n)=\mathrm{Id}(\{a\})=M$. ■

385 ~ 386

我们继续研究算子 Var 和 Id.

命题 6.103 设 k 是任意域.

(i) 对每个子集 $F\subseteq k^n$，

$$\mathrm{Var}(\mathrm{Id}(F))\supseteq F.$$

(ii) 对每个理想 $I\subseteq k[X]$，

$$\mathrm{Id}(\mathrm{Var}(I))\supseteq I.$$

(iii) 如果 V 是 k^n 的簇，则 $\mathrm{Var}(\mathrm{Id}(V))=V$.

(iv) 如果 F 是 k^n 的子集，则 $\overline{F}$（一切包含 F 的簇的交）等于 $\mathrm{Var}(\mathrm{Id}(F))$. 称 $\overline{F}$ 为 F 的扎里斯基闭包[⊖].

(v) 如果 $V\subseteq V^*\subseteq k^n$ 是簇，则

$$V^*=V\cup\overline{V^*-V},$$

$\overline{V^*-V}$ 是 V^*-V 的扎里斯基闭包.

证明 (i) 这个结果几乎是同语反复. 如果 $a\in F$，则对一切 $g(X)\in\mathrm{Id}(F)$ 有 $g(a)=0$. 但由 $\mathrm{Id}(F)$ 的定义，每个 $g(X)\in\mathrm{Id}(F)$ 在 F 上是零，从而 $a\in\mathrm{Var}(\mathrm{Id}(F))$. 所以 $\mathrm{Var}(\mathrm{Id}(F))\supseteq F$.

(ii) 我们也只需看定义. 如果 $f(X)\in I$，则对一切 $a\in\mathrm{Var}(I)$ 有 $f(a)=0$，因此 $f(X)$ 确实是在 $\mathrm{Var}(I)$ 上零化的多项式之一.

(iii) 如果 V 是簇，则有 $k[X]$ 中的某个理想 J 使得 $V=\mathrm{Var}(J)$. 现在根据 (i)，

$$\mathrm{Var}(\mathrm{Id}(\mathrm{Var}(J)))\supseteq\mathrm{Var}(J).$$

(ii) 也给出 $\mathrm{Id}(\mathrm{Var}(J))\supseteq J$，运用命题 6.92(i) 得反包含

$$\mathrm{Var}(\mathrm{Id}(\mathrm{Var}(J)))\subseteq\mathrm{Var}(J).$$

所以 $\mathrm{Var}(\mathrm{Id}(\mathrm{Var}(J)))=\mathrm{Var}(J)$，即 $\mathrm{Var}(\mathrm{Id}(V))=V$.

(iv) 根据命题 6.93(iii)，$\overline{F}=\bigcap_{V\supseteq F}V$ 是包含 F 的簇. 因 $\mathrm{Var}(\mathrm{Id}(F))$ 是包含 F 的簇，它是形成 $\overline{F}$ 的交中那些簇 V 的一个，从而 $\overline{F}\subseteq\mathrm{Var}(\mathrm{Id}(F))$. 关于反包含，只要证明如果 V 是包含 F 的任意簇，则 $V\supseteq\mathrm{Var}(\mathrm{Id}(F))$. 如果 $V\supseteq F$，则 $\mathrm{Id}(V)\subseteq\mathrm{Id}(F)$，且 $V=\mathrm{Var}(\mathrm{Id}(V))\supseteq\mathrm{Var}(\mathrm{Id}(F))$.

(v) 因 $V^*-V\subseteq V^*$，有 $\overline{V^*-V}\subseteq\overline{V^*}=V^*$. 根据假设，$V\subseteq V^*$，从而 $V\cup\overline{V^*-V}\subseteq$

⊖ 如果 F 是拓扑空间 X 的子集，则它的闭包定义为 X 中包含 F 的一切闭集的交.

V^*. 关于反包含，有子集等式 $V^* = V \cup (V^* - V)$. 取闭包，因为 $V = \overline{V}$，有

387

$$V^* = \overline{V^*} = \overline{V} \cup \overline{V^* - V} = V \cup \overline{V^* - V}.$$

■

系 6.104 （ⅰ）如果 V_1 和 V_2 都是簇，且 $\mathrm{Id}(V_1) = \mathrm{Id}(V_2)$，则 $V_1 = V_2$.

（ⅱ）设 k 是（不可数）代数闭域. 如果 I_1 和 I_2 都是根理想，且 $\mathrm{Var}(I_1) = \mathrm{Var}(I_2)$，则 $I_1 = I_2$.

证明 （ⅰ）如果 $\mathrm{Id}(V_1) = \mathrm{Id}(V_2)$，则 $\mathrm{Var}(\mathrm{Id}(V_1)) = \mathrm{Var}(\mathrm{Id}(V_2))$，由命题 6.103(ⅲ) 得 $V_1 = V_2$.

（ⅱ）如果 $\mathrm{Var}(I_1) = \mathrm{Var}(I_2)$，则 $\mathrm{Id}(\mathrm{Var}(I_1)) = \mathrm{Id}(\mathrm{Var}(I_2))$. 因为 k 是（不可数）代数闭域，零点定理成立，由此 $\sqrt{I_1} = \sqrt{I_2}$. 根据假设，I_1 和 I_2 都是根理想，所以 $I_1 = I_2$. ■

一个簇能够分解为较简单的子簇吗？

定义 如果簇 V 不是两个真子簇的并；即 $V \neq W' \cup W''$，其中 W' 和 W'' 都是簇且都是 V 的真子集，则称簇 V 是**不可约的**.

命题 6.105 k^n 中的每个簇 V 都是有限个不可约子簇的并：

$$V = V_1 \cup V_2 \cup \cdots \cup V_m.$$

证明 称簇 $W \subseteq k^n$ 是好的，如果它是不可约的或是有限个不可约子簇的并，否则称 W 是坏的. 我们需要证明没有坏簇. 如果 W 是坏的，则它不是不可约的，从而 $W = W' \cup W''$，其中 W' 和 W'' 都是真子簇. 但好簇的并也是好簇，从而 W' 和 W'' 中至少有一个是坏的，比如 W' 是坏的，重命名 $W' = W_1$. 对于 W_1 重复这个构造方法得到坏子簇 W_2. 由归纳法可知存在坏子簇的严格递减序列

$$W \supsetneq W_1 \supsetneq \cdots \supsetneq W_n \supsetneq \cdots.$$

因算子 Id 反转包含关系，所以存在理想的严格升链

$$\mathrm{Id}(W) \subsetneq \mathrm{Id}(W_1) \subsetneq \cdots \subsetneq \mathrm{Id}(W_n) \subsetneq \cdots$$

[根据系 6.104(ⅰ)，包含关系是严格的]，此与希尔伯特基定理矛盾. 由此可知每个簇都是好的.

■

不可约簇有一个好的刻画.

命题 6.106 k^n 中的簇 V 是不可约的当且仅当 $\mathrm{Id}(V)$ 是 $k[X]$ 中的素理想. 因此，不可约簇 V 的坐标环 $k[V]$ 是整环.

证明 假定 V 是不可约簇. 只要证明如果 $f_1(X), f_2(X) \notin \mathrm{Id}(V)$，则 $f_1(X)f_2(X) \notin \mathrm{Id}(V)$. 对 $i = 1,2$ 定义

388

$$W_i = V \cap \mathrm{Var}(f_i(X)).$$

注意，因为每个 W_i 都是两个簇的交，所以都是 V 的子簇. 此外，因 $f_i(X) \notin \mathrm{Id}(V)$，有某个 $a_i \in V$ 使得 $f_i(a_i) \neq 0$，从而 W_i 是 V 的真子簇. 因 V 是不可约的，不可能有 $V = W_1 \cup W_2$. 于是存在某个 $b \in V$ 不在 $W_1 \cup W_2$ 中，即 $f_1(b) \neq 0 \neq f_2(b)$. 所以 $f_1(b)f_2(b) \neq 0$，因此 $f_1(X)f_2(X) \notin Id(V)$，从而 $\mathrm{Id}(V)$ 是素理想.

反之，假定 $\mathrm{Id}(V)$ 是素理想. 假设 $V = V_1 \cup V_2$，其中 V_1 和 V_2 都是子簇. 如果 $V_2 \subsetneq V$，则需要证明 $V = V_1$. 现在

$$\mathrm{Id}(V) = \mathrm{Id}(V_1) \cap \mathrm{Id}(V_2) \supseteq \mathrm{Id}(V_1)\,\mathrm{Id}(V_2);$$

其中等式由命题 6.96 给出，不等式由习题 6.10 给出. 因 $\mathrm{Id}(V)$ 是素理想，命题 6.13 说 $\mathrm{Id}(V_1) \subseteq \mathrm{Id}(V)$ 或 $\mathrm{Id}(V_2) \subseteq \mathrm{Id}(V)$. 但 $V_2 \subsetneq V$ 蕴涵 $\mathrm{Id}(V_2) \supsetneq \mathrm{Id}(V)$，由此可知 $\mathrm{Id}(V_1) \subseteq \mathrm{Id}(V)$. 现在因

为 $V_1 \subseteq V$，反过来的不等式 $\mathrm{Id}(V_1) \supseteq \mathrm{Id}(V)$ 也成立，从而 $\mathrm{Id}(V_1) = \mathrm{Id}(V)$. 所以，根据系 6.104，$V = V_1$，因此 V 是不可约的. ■

我们现在考虑一个簇分解为不可约子簇的并时，那些不可约子簇是否是唯一确定的. 有一种明显的方法可以使得这种分解不唯一. 如果在 $k[X]$ 中 $P \subsetneq Q$ 是两个素理想（例如，$(x) \subsetneq (x,y)$ 就是 $k[x,y]$ 中这样的素理想），则 $\mathrm{Var}(Q) \subsetneq \mathrm{Var}(P)$. 如果 $\mathrm{Var}(P)$ 是簇 V 的子簇，比如 $V = \mathrm{Var}(P) \cup V_2 \cup \cdots \cup V_m$，则 $\mathrm{Var}(Q)$ 可以是 V_i 中的一个，也可以没有它.

定义 分解 $V = V_1 \cup \cdots \cup V_m$ 称为**无赘并**，如果没有一个 V_i 可以略去，即对一切 i，

$$V \neq V_1 \cup \cdots \cup \hat{V}_i \cup \cdots \cup V_m.$$

命题 6.107 每个簇 V 都是不可约子簇的无赘并

$$V = V_1 \cup \cdots \cup V_m;$$

此外，不可约子簇 V_i 被 V 唯一确定.

证明 根据命题 6.105，V 是有限个不可约子簇的并，比如 $V = V_1 \cup \cdots \cup V_m$. 如果选取 m 为极小，则这个并必定是无赘的.

现在证明唯一性. 假设 $V = W_1 \cup \cdots \cup W_s$ 是不可约子簇的无赘并. 设 $X = \{V_1, \cdots, V_m\}$ 和 $Y = \{W_1, \cdots, W_s\}$，我们将证明 $X = Y$. 如果 $V_i \in X$，我们有

$$V_i = V_i \cap V = \bigcup_j (V_i \cap W_j).$$

现在有某个 j 使得 $V_i \cap W_j \neq \varnothing$，因 V_i 是不可约的，这样的 W_j 只有一个. 所以 $V_i = V_i \cap W_j$，从而 $V_i \subseteq W_j$. 把同样的论证运用到 W_j 表明恰有一个 V_ℓ 使得 $W_j \subseteq V_\ell$. 因此，

$$V_i \subseteq W_j \subseteq V_\ell.$$

389

因并 $V_1 \cup \cdots \cup V_m$ 是无赘的，必有 $V_i = V_\ell$，从而 $V_i = W_j = V_\ell$，即 $V_i \in Y$ 和 $X \subseteq Y$. 用同样的方法可以证明反过来的包含关系. ■

定义 一个交 $I = J_1 \cap \cdots \cap J_m$ 称为**无赘的**，如果没有一个 J_i 可以略去，即对一切 i，

$$I \neq J_1 \cap \cdots \cap \hat{J}_i \cap \cdots \cap J_m.$$

系 6.108 如果 k 是代数闭的，则 $k[X]$ 中的每个根理想 J 都是素理想的无赘交，

$$J = P_1 \cap \cdots \cap P_m;$$

此外，素理想 P_i 被 J 唯一确定.

注 习题 6.72 推广了这个系：任意交换诺特环中的理想是根理想当且仅当它是有限个素理想的交.

证明 因 J 是根理想，存在簇 V 使得 $J = \mathrm{Id}(V)$. 现在 V 是不可约子簇的无赘并，

$$V = V_1 \cup \cdots \cup V_m,$$

从而

$$J = \mathrm{Id}(V) = \mathrm{Id}(V_1) \cap \cdots \cap \mathrm{Id}(V_m).$$

根据命题 6.106，V_i 不可约蕴涵 $\mathrm{Id}(V_i)$ 是素的，从而 J 是素理想的交. 这个交是无赘的，因为如果存在 ℓ 使得 $J = \mathrm{Id}(V) = \bigcap_{j \neq \ell} \mathrm{Id}(V_j)$，则

$$V = \mathrm{Var}(\mathrm{Id}(V)) = \bigcup_{j \neq \ell} \mathrm{Var}(\mathrm{Id}(V_j)) = \bigcup_{j \neq \ell} V_j,$$

与给定的并的无赘性矛盾.

唯一性的证明是类似的. 如果 $J = \mathrm{Id}(W_1) \cap \cdots \cap \mathrm{Id}(W_s)$，其中每个 $\mathrm{Id}(W_i)$ 都是素理想

(因此是根理想),则每个 W_i 都是不可约簇. 应用 Var,把 $V = \mathrm{Var}(\mathrm{Id}(V)) = \mathrm{Var}(J)$ 表示为不可约子簇的无赘并,这个分解的唯一性给出交中素理想的唯一性. ■

给定 $k[x_1,\cdots,x_n]$ 中的理想 I,如何求得 $\mathrm{Var}(I)$ 的不可约成分 C_i?该问题换成另一种问法,什么样的素理想 P_i 能够使得 $C_i = \mathrm{Var}(P_i)$?最先的猜想是 $I = P_1 \cap \cdots \cap P_r$,但易知这是错的:存在不是素理想的交的理想 I. 例如,在 $k[x]$ 中,理想 $((x-1)^2)$ 就不是素理想的交. 依据零点定理,可以把素理想 P_i 替换为满足 $\sqrt{Q_i} = P_i$ 的理想 Q_i,这是由于 $\mathrm{Var}(P_i) = \mathrm{Var}(Q_i)$. 这引导我们立即定义准素理想的概念和准素分解定理,它说在交换诺特环中而不仅仅在 $k[X]$ 中,每个理想都是准素理想的交.

390

我们现在可以给出冒号理想的一个几何解释.

命题 6.109 设 k 是(不可数)代数闭域,并设 I 是 $k[X]$ 中的根理想. 则对每个理想 J,

$$\mathrm{Var}((I:J)) = \overline{\mathrm{Var}(I) - \mathrm{Var}(J)}.$$

证明 先证明 $\mathrm{Var}((I:J)) \supseteq \overline{\mathrm{Var}(I) - \mathrm{Var}(J)}$. 如果 $f \in (I:J)$,则对一切 $g \in J$,$fg \in I$. 因此,如果 $x \in \mathrm{Var}(I)$,则对一切 $g \in J$,$f(x)g(x) = 0$. 然而,如果 $x \notin \mathrm{Var}(J)$,则有 $g \in J$ 使得 $g(x) \neq 0$. 因 $k[X]$ 是整环,所以对一切 $x \in \mathrm{Var}(I) - \mathrm{Var}(J)$ 有 $f(x) = 0$;即 $f \in \mathrm{Id}(\mathrm{Var}(I) - \mathrm{Var}(J))$. 于是 $(I:J) \subseteq \mathrm{Id}(\mathrm{Var}(I) - \mathrm{Var}(J))$,从而根据命题 6.103(iv),

$$\mathrm{Var}((I:J)) \supseteq \mathrm{Var}(\mathrm{Id}(\mathrm{Var}(I) - \mathrm{Var}(J))) = \overline{\mathrm{Var}(I) - \mathrm{Var}(J)}.$$

关于反包含,取 $x \in \mathrm{Var}((I:J))$. 于是,如果 $f \in (I:J)$,则 $f(x) = 0$;即

$$\text{如果对一切 } g \in J \text{ 有 } fg \in I,\text{ 则 } f(x) = 0.$$

现在假设 $h \in \mathrm{Id}(\mathrm{Var}(I) - \mathrm{Var}(J))$. 如果 $g \in J$,则 hg 在 $\mathrm{Var}(J)$ 上变成零(因为 g 变成零);另一方面,hg 在 $\mathrm{Var}(I) - \mathrm{Var}(J)$ 上变成零(因为 h 变成零). 由此,hg 在 $\mathrm{Var}(J) \cup (\mathrm{Var}(I) - \mathrm{Var}(J)) = \mathrm{Var}(I)$ 上变成零. 因为 I 是根理想,所以对一切 $g \in J$,$hg \in \sqrt{I} = I$,从而 $h \in (I:J)$. 由此,对一切 $h \in (I:J)$,$h(x) = 0$,因而给出所要的 $x \in \mathrm{Var}(\mathrm{Id}(\mathrm{Var}(I) - \mathrm{Var}(J))) = \overline{\mathrm{Var}(I) - \mathrm{Var}(J)}$. ■

定义 交换环 R 中的理想 Q 称为**准素的**,如果它是真理想且对任意的 $ab \in Q$(其中 $a,b \in R$)和 $b \notin Q$,必有某个 $n \geqslant 1$ 使得 $a^n \in Q$.

显然每个素理想都是准素的. 此外,在 $\mathbb{Z}$ 中,理想 (p^e) 是一个不是素理想的准素理想,其中 p 是素数且 $e \geqslant 2$. 例 6.114 表明这个例子使我们产生错误的印象:存在不是素理想幂的准素理想,又存在不是准素理想的素理想幂.

命题 6.110 如果 Q 是准素理想,则它的根 $P = \sqrt{Q}$ 是素理想. 此外,如果 Q 是准素的,则 $ab \in Q$ 和 $a \notin Q$ 蕴涵 $b \in P$.

证明 假定 $ab \in \sqrt{Q}$,于是有某个 $m \geqslant 1$ 使得 $(ab)^m = a^m b^m \in Q$. 如果 $a \notin \sqrt{Q}$,则 $a^m \notin Q$. 因 Q 是准素的,从而有 b^m 的某个幂,比如 $b^{mn} \in Q$,即 $b \in \sqrt{Q}$. 由此证明了 $\sqrt{Q}$ 是素的,且第二个陈述成立. ■

如果 Q 是准素的且 $P = \sqrt{Q}$,则我们常称 Q 是 P-**准素理想**,并说 Q 和 P 相互**从属**.

391

现在证明命题 6.110 中的性质刻画了准素理想.

命题 6.111 设 J 和 T 是交换环中的理想. 如果(i)$J \subseteq T$,(ii)$t \in T$ 蕴涵存在某个 $m \geqslant 1$ 使得 $t^m \in J$,(iii)如果 $ab \in J$ 和 $a \notin J$,有 $b \in T$,则 J 是以 T 为根的准素理想.

证明 首先,如果 $ab \in J$ 和 $a \notin J$,则公理(iii)给出 $b \in T$,公理(ii)给出 $b^m \in J$,从

而 J 是准素理想．剩下要证明 $T=\sqrt{J}$．现在公理（ii）给出 $T\subseteq\sqrt{J}$．关于反包含，如果 $r\in\sqrt{J}$，则 $r^m\in J$，选取 m 极小．如果 $m=1$，则公理（i）给出所要的 $r\in J\subseteq T$．如果 $m>1$，则 $rr^{m-1}\in J$，因 $r^{m-1}\notin J$，公理（iii）给出 $r\in T$．所以 $T=\sqrt{J}$． ■

设 R 是交换环，并设 M 是理想．每个 $a\in R$ 由 $a_M: m\mapsto am$ 定义了一个 R-映射 $a_M: M\to M$.

引理 6.112 设 Q 是交换环 R 中的理想，则 Q 是准素理想当且仅当对每个 $a\in R$，由 $r+Q\mapsto ar+Q$ 给出的映射 $a_{R/Q}: R/Q\to R/Q$ 是单射或是幂零映射［对某个 $n\geqslant 1$ 有 $(a_{R/Q})^n=0$］．

证明 假定 Q 是准素的．如果 $a\in R$ 且 $a_{R/Q}$ 不是单射，则存在 $b\in R$ 满足 $b\notin Q$ 及 $a_{R/Q}(b+Q)=ab+Q=Q$；即 $ab\in Q$．我们需要证明 $a_{R/Q}$ 是幂零的．因 Q 是准素的，存在 $n\geqslant 1$ 使得 $a^n\in Q$，因为 Q 是理想，所以对一切 $r\in R$ 有 $a^nr\in Q$．于是对一切 $r\in R$，$(a_{R/Q})^n(r+Q)=a^nr+Q=Q$，从而 $(a_{R/Q})^n=0$；即 $a_{R/Q}$ 是幂零的．

反之，假定每个 $a_{R/Q}$ 或者是单射或者是幂零的．假设 $ab\in Q$ 且 $a\notin Q$，则因 $a+Q\in\ker b_{R/Q}$，所以 $b_{R/Q}$ 不是单射．根据假设，有某个 $n\geqslant 1$ 使得 $(b_{R/Q})^n=0$；即对一切 $r\in R$，$b^nr\in Q$．令 $r=1$ 得 $b^n\in Q$，因此 Q 是准素的． ■

下一结果给出准素理想的构造方法．

命题 6.113 如果 P 是交换环 R 中的极大理想，且 Q 是一个理想满足对某个 $e\geqslant 0$ 有 $P^e\subseteq Q\subseteq P$，则 Q 是 P-准素理想．特别地，每个极大理想的幂都是准素理想．

证明 对每个 $a\in R$，我们证明 $a_{R/Q}$ 是幂零的或是单射．先假设 $a\in P$．此时，$a^e\in P^e\subseteq Q$，因此对一切 $b\in R$，$a^eb\in Q$，从而 $(a_{R/Q})^e=0$；即 $a_{R/Q}$ 是幂零的．现在假定 $a\notin P$，我们要证明 $a+Q$ 是 R/Q 中的单位，这蕴涵 $a_{R/Q}$ 是单射．因 P 是极大理想，环 R/P 是域；因 $a\notin P$，元素 $a+P$ 是 R/P 中的单位：存在 $a'\in R$ 和 $z\in P$ 使得 $aa'=1-z$．现在因为 $z^e\in P^e\subseteq Q$，所以 $z+Q$ 是 R/Q 的幂零元素，于是 $1-z+Q$ 是 R/Q 中的单位（它的逆是 $1+z+\cdots+z^{e-1}$）．因为 $aa'+Q=1-z+Q$，所以 $a+Q$ 是 R/Q 中的单位．现在由引理 6.112 可知 Q 是准素理想．最后，因为 $P=\sqrt{P^e}\subseteq\sqrt{Q}\subseteq\sqrt{P}=P$，所以 Q 从属于 P． ■

例 6.114 （i）我们现在证明素理想的幂未必是准素的．假设 R 是交换环包含元素 a,b,c 满足 $ab=c^2$，$P=(a,c)$ 是素理想，$a\notin P^2$ 和 $b\notin P$．现在 $ab=c^2\in P^2$，如果 P^2 是准素的，则 $a\in P^2$ 蕴涵 $b\in\sqrt{P^2}=P$，但 $b\notin P$．我们如下构造这样一个环 R．设 k 是域，定义 $R=k[x,y,z]/(xy-z^2)$（注意 R 是诺特环）．定义 $a,b,c\in R$ 分别为 x,y,z 的陪集．现在由环的第三同构定理，$P=(a,c)$ 是素理想．习题 3.82 给出 392

$$R/(a,c)=\frac{k[x,y,z]/(xy-z^2)}{(x,z)/(xy-z^2)}\cong\frac{k[x,y,z]}{(x,z)}\cong k[y],$$

这是一个域．等式 $ab=c^2$ 在 R 中显然成立．如果 $a\in P^2$，则提升这一关系到 $k[x,y,z]$ 产生等式

$$x=f(x,y,z)x^2+g(x,y,z)xz+h(x,y,z)z^2+\ell(x,y,z)(xy-z^2).$$

令 $y=0=z$（即运用赋值同态 $k[x,y,z]\to k[x]$）得到 $k[x]$ 中的等式 $x=f(x,0,0)x^2$，产生矛盾．类似的推论可证明 $b\notin P$．

（ii）我们用命题 6.113 证明存在不是素理想之幂的准素理想 Q．设 $R=k[x,y]$，其中 k 是域．理想 $P=(x,y)$ 是极大理想，因此是素理想（因为 $R/P\cong k$）．此外，

$$P^2\subsetneq(x^2,y)\subsetneq(x,y)=P$$

[由 $x \notin (x^2,y)$ 和 $y \notin P^2$ 得严格不等性]. 于是 $Q=(x^2,y)$ 不是 P 的幂，确实，我们证明 $Q \neq L^e$，其中 L 是一个素理想. 如果 $Q=L^e$，则 $P^2 \subseteq L^e \subseteq P$，因此 $\sqrt{P^2} \subseteq \sqrt{L^e} \subseteq \sqrt{P}$，从而 $P \subseteq L \subseteq P$，这是一个矛盾. ■

我们现在推广系 6.108，证明在诺特环中，特别是在 $k[x]$ 中（其中 k 是域）每个理想都是准素理想的交. 这个结果和唯一性一起，最先由拉斯克（E. Lasker）证明；后来诺特简化了他的证明. 注意我们是对任意诺特环进行证明，而不仅仅是 $k[x]$.

定义 交换环 R 中的理想 I 的一个**准素分解**是指有一个准素理想的有限族 $Q_1,\cdots,Q_r$ 使得

$$I = Q_1 \cap Q_2 \cap \cdots \cap Q_r.$$

定理 6.115（拉斯克-诺特 Ⅰ） 如果 R 是交换诺特环，则 R 中的每个真理想 I 都有准素分解.

证明 设$\mathcal{F}$是 R 中一切没有准素分解的真理想的族，我们需要证明$\mathcal{F}$是空集. 因 R 是诺特环，如果$\mathcal{F} \neq \varnothing$，则它有极大元素，比如 J. 当然 J 不是准素的，因此存在 $a \in R$ 使得 $a_{R/J}: R/J \to R/J$ 既不是单射也不是幂零的. R/J 的理想的升链

393

$$\ker a_{R/J} \subseteq \ker (a_{R/J})^2 \subseteq \ker (a_{R/J})^3 \subseteq \cdots$$

必有终止（因为 R/J 是诺特环的商，也是诺特环），从而存在 $m \geqslant 1$ 使得对于一切 $\ell \geqslant m$ 有 $\ker (a^{\ell}_{R/J}) = \ker (a^m_{R/J})$. 记 $(a_{R/J})^m$ 为 φ，于是 $\ker (\varphi^2) = \ker\varphi$. 注意，因为 $\{0\} \subsetneq \ker a_{R/J} \subseteq \ker (a_{R/J})^m = \ker\varphi$，所以 $\ker\varphi \neq \{0\}$，且因 $a_{R/J}$ 不是幂零的，所以 $\mathrm{im}\varphi = \mathrm{im}\,(a_{R/J})^m \neq \{0\}$. 我们断言

$$\ker \varphi \cap \mathrm{im}\, \varphi = \{0\}.$$

如果 $x \in \ker\varphi \cap \mathrm{im}\varphi$，则 $\varphi(x)=0$ 且有某个 $y \in R/J$ 使得 $x=\varphi(y)$. 但 $\varphi(x)=\varphi(\varphi(y))=\varphi^2(y)$，从而 $y \in \ker(\varphi^2)=\ker\varphi$ 和 $x=\varphi(y)=0$.

如果 $\pi: R \to R/J$ 是自然映射，则 $A=\pi^{-1}(\ker\varphi)$ 和 $A'=\pi^{-1}(\mathrm{im}\varphi)$ 是 R 的理想满足 $A \cap A' = J$. 显然 A 是真理想，我们断言 A' 也是真理想. 否则 $A'=R$，从而 $A \cap A' = A$，但在上面已经看到 $A \cap A' = J$ 和 $A \neq J$，这是一个矛盾. 因 A 和 A' 都严格大于 J，所以它们都不在$\mathcal{F}$中：存在准素分解 $A = Q_1 \cap \cdots \cap Q_m$ 和 $A' = Q'_1 \cap \cdots \cap Q'_n$，因此

$$J = A \cap A' = Q_1 \cap \cdots \cap Q_m \cap Q'_1 \cap \cdots \cap Q'_n,$$

这与 J 没有准素分解矛盾（因为 $J \in \mathcal{F}$）. ■

定义 准素分解 $I = Q_1 \cap \cdots \cap Q_r$ 称为**无赘的**，如果没有一个 Q_i 可被略去；即对一切 i，

$$I \neq Q_1 \cap \cdots \cap \hat{Q}_i \cap \cdots \cap Q_r.$$

素理想 $P_1=\sqrt{Q_1},\cdots,P_r=\sqrt{Q_r}$ 叫做这个无赘准素分解的**相伴素理想**.

显然只要一个一个地丢弃包含其他准素理想之交的准素理想，便可得到无赘分解.

定理 6.116（拉斯克-诺特 Ⅱ） 如果 I 是诺特环 R 中的理想，则 I 的任意两个无赘准素分解有相同的相伴素理想集. 因此，相伴素理想由 I 唯一确定.

证明 设 $I = Q_1 \cap \cdots \cap Q_r$ 是无赘准素分解，并设 $P_i = \sqrt{Q_i}$. 我们要证明 R 中的一个素理想 P 等于某个 P_i 当且仅当存在 $c \notin I$ 使得 $(I:c)$ 是一个 P-准素理想，证明了这一点就足够了，因为冒号理想 $(I:c)$ 仅由 I 定义，不牵涉到任何准素分解.

给定 P_i，因无赘性，存在 $c \in \bigcap_{j \neq i} Q_j$ 且 $c \notin Q_i$，我们证明 $(I:c)$ 是 P_i-准素理想. 回忆命题

6.111：如果下列三条件成立则 $(I:c)$ 是 P_i-准素的：：（ⅰ）$(I:c)\subseteq P_i$；（ⅱ）$b\in P_i$ 蕴涵存在某个 $m\geq 1$ 使得 $b^m\in(I:c)$；（ⅲ）如果 $ab\in(I:c)$ 和 $a\notin(I:c)$，则 $b\in P_i$.

证（ⅰ）. 如果 $u\in(I:c)$，则 $uc\in I\subseteq P_i$. 因 $c\notin Q_i$，根据命题 6.110，$u\in P_i$. 为证（ⅱ），我们先证明 $Q_i\subseteq(I:c)$. 如果 $a\in Q_i$，则因 Q_i 是理想，所以有 $ca\in Q_i$. 如果 $j\neq i$，则 $c\in Q_j$，从而 $ca\in Q_j$. 所以 $ca\in Q_1\cap\cdots\cap Q_r=I$，因此 $a\in(I:c)$. 现在如果 $b\in P_i$，则 $b^m\in Q_i\subseteq(I:c)$. 最后，我们证明（ⅲ）的逆否命题：如果 $xy\in(I:c)$ 且 $x\notin P_i$，则 $y\in(I:c)$. 假定 $xyc\in I$；因 $I\subseteq Q_i$ 且 $x\notin P_i=\sqrt{Q_i}$，所以有 $yc\in Q_i$. 但对一切 $j\neq i$，因 $c\in Q_j$，所以有 $yc\in Q_j$. 因此 $yc\in Q_1\cap\cdots\cap Q_r=I$，从而 $y\in(I:c)$. 由此可知 $(I:c)$ 是 P_i-准素的.

394

反之，假定存在元素 $c\notin I$ 和素理想 P 使得 $(I:c)$ 是 P-准素的. 我们需要证明有某个 i 使得 $P=P_i$. 习题6.14(ⅱ)给出 $(I:c)=(Q_1:c)\cap\cdots\cap(Q_r:c)$，所以根据命题 6.98,

$$P=\sqrt{(I:c)}=\sqrt{(Q_1:c)}\cap\cdots\cap\sqrt{(Q_r:c)}.$$

如果 $c\in Q_i$，则 $(Q_i:c)=R$；如果 $c\notin Q_i$，则在这个证明的第一部分中我们看到 $(Q_i:c)$ 是 P_i-准素的. 于是存在 $s\leq r$ 使得

$$P=\sqrt{(Q_{i_1}:c)}\cap\cdots\cap\sqrt{(Q_{i_s}:c)}=P_{i_1}\cap\cdots\cap P_{i_s}.$$

当然对一切 j 有 $P\subseteq P_{i_j}$. 另一方面，由习题6.10(ⅲ)，存在某个 j 使得 $P_{i_j}\subseteq P$，因此正如所要的 $P=P_{i_j}$. ■

例 6.117 （ⅰ）设 $R=\mathbb{Z}$, (n) 是非零真理想，并设 $n=p_1^{e_1}\cdots p_t^{e_t}$ 是素因数分解. 则

$$(n)=(p_1^{e_1})\cap\cdots\cap(p_t^{e_t})$$

是一个无赘准素分解.

（ⅱ）设 $R=k[x,y]$，其中 k 是域. 定义 $Q_1=(x)$ 和 $Q_2=(x,y)^2$. 注意 Q_1 是素理想，因此对 $P_1=Q_1$，Q_1 是 P_1-准素理想. 而且，$P_2=(x,y)$ 是极大理想，从而根据命题 6.113，$Q_2=P_2^2$ 是 P_2-准素的. 定义 $I=Q_1\cap Q_2$. I 的这个准素分解是无赘的. I 的相伴素理想是 $\{P_1,P_2\}$. ■

有一个描述正规化的准素分解的第二种唯一结果，但我们先给出一个引理.

引理 6.118 *如果 P 是素理想且 $Q_1,\cdots,Q_n$ 是 P-准素理想，则 $Q_1\cap\cdots\cap Q_n$ 也是 P-准素理想.*

证明 对 $I=Q_1\cap\cdots\cap Q_n$ 验证命题 6.111 假设中的三项成立. 显然 $I\subseteq P$. 其次，如果 $b\in P$，则对一切 i，因 Q_i 是 P-准素的，有 $b^{m_i}\in Q_i$. 因此 $b^m\in I$，其中 $m=\max\{m_1,\cdots,m_n\}$. 最后，假定 $ab\in I$. 如果 $a\notin I$，则有某个 i 使得 $a\notin Q_i$. 因 Q_i 是 P-准素的，$ab\in I\subseteq Q_i$ 和 $a\notin Q_i$ 蕴涵 $b\in P$. 所以 I 是 P-准素的. ■

定义 *准素分解 $I=Q_1\cap\cdots\cap Q_r$ 称为***正规的***，如果它是无赘的且一切素理想 $P_i=\sqrt{Q_i}$ 都不同.*

395

系 6.119 *如果 R 是诺特环，则 R 中的每个真理想都有正规准素分解.*

证明 根据定理 6.115，每个真理想都有准素分解，比如

$$I=Q_1\cap\cdots\cap Q_r,$$

其中 Q_i 是 P_i-准素的. 如果对某个 $i<r$ 有 $P_r=P_i$，则 Q_i 和 Q_r 可以被 $Q'=Q_i\cap Q_r$ 替代，根据引理 6.118，Q' 也是准素的. 进行迭代，最终得到一切素理想都不同的准素分解. 如果这个分解不是无赘的，则从中一个一个移去准素理想以得到正规准素分解. ■

定义 *如果 $I=Q_1\cap\cdots\cap Q_r$ 是正规准素分解，则极小素理想 $P_i=\sqrt{Q_i}$ 称为***孤立素理想***，其*

他的素理想（如果有的话）称为**嵌入素理想**.

在例6.117(ⅱ)中，我们给出 $k[x,y]$ 中的一个无赘准素分解 $I=(x)\cap(x,y)^2$，其中 k 是域. 相伴素理想是 (x) 和 (x,y)，从而 (x) 是一个孤立素理想，(x,y) 是一个嵌入素理想.

定义 素理想 P 称为在理想 I 上**极小**，如果 $I\subseteq P$ 且没有素理想 P' 满足 $I\subseteq P'\subsetneq P$.

系 6.120 设 I 是诺特环 R 中的理想.

(ⅰ) I 的任意两个正规准素分解有相同的孤立素理想集，从而孤立素理想由 I 唯一确定.

(ⅱ) I 只有有限个极小素理想.

(ⅲ) 一个诺特环只有有限个极小素理想.

证明 (ⅰ) 设 $I=Q_1\cap\cdots\cap Q_n$ 是正规准素分解. 如果 P 是任一包含 I 的素理想，则

$$P\supseteq I=Q_1\cap\cdots\cap Q_n\supseteq Q_1\cdots Q_n.$$

现在根据命题 6.13，对某个 i 有 $P\supseteq Q_i$，从而 $P\supseteq\sqrt{Q_i}=P_i$. 换句话说，包含 I 的任一素理想必包含一个孤立相伴素理想. 因此孤立素理想是 I 的相伴素理想集合中的极小元素，根据定理 6.116，它由 I 唯一确定.

(ⅱ) 和 (ⅰ) 一样，包含 I 的任一素理想 P 必包含 I 的一个孤立素理想. 因此，如果 P 在 I 上是极小的，则 P 必定等于 I 的一个孤立素理想. 因为 I 只有有限个孤立素理想，所以结论成立.

396

(ⅲ) 取 $I=\{0\}$，由 (ⅱ) 得结论. ■

深入研究这些理想会产生一些自然的问题. 首先，一个簇的维数是什么? 有几个候选者，而关键是素理想. 如果 V 是簇，则它的维数是它的坐标环 $k[V]$ 中最长素理想链的长度（由对应定理，它是 $k[X]$ 中 $\mathrm{Id}(V)$ 上的最长素理想链的长度）.

在 k^n 中添加一个"无穷远处的超平面"形成较大的**射影空间**可以使得研究工作更为方便. 例如，在通常平面中添加一条无穷远处的直线形成射影平面（它是"水平线"，一切平行线在那里相交）. 为了和射影空间相区别，把 k^n 叫**仿射空间**，因为它由一切"有限点"组成——即没有点在无穷远处. 如果我们在射影空间中研究簇，现在簇被定义为齐次多项式集合的零点，则常常出现这种情况：在仿射空间中许多分散的情形变成单一射影公式的一部分. 例如，定义 $\deg(C)$ 为 $C\cap\ell$ 中点的最多个数，其中 ℓ 是直线. 如果 $C=\mathrm{Var}(f)$ 是 d 次多项式形成的曲线，我们希望 $\deg(C)=d$，但是这里有几个问题. 第一，必须要求系数域是代数闭的，否则引起 $\mathrm{Var}(f)=\varnothing$ 的问题. 第二，可能有重根，因此有些交可能必须计算某种*重数*. *贝祖定理*说，如果 C 和 C' 是两条曲线，则 $|C\cap C'|=\deg(C)\deg(C')$. 这个公式在射影空间中成立，但在仿射簇中可能不成立. 对高维簇的交定义重数是十分深奥的.

第三，微分流形和簇极为相似. 一个*流形*是$\mathbb{R}^n$ 的子空间，它是欧几里得空间的开仿样的并. 例如，环面 T（即圆环面）是$\mathbb{R}^3$ 的子空间，T 的每个点有类似于开圆盘的邻域（它与平面同胚）. 我们说 T 是"局部欧几里得的"，它是把$\mathbb{R}^2$ 的复制连续地黏合在一起而得到的. 一个流形是可微的是指它的每个点都有切平面. 一个簇 V 可以看作它的坐标环 $k[V]$，它的点的邻域可以用局部环的所谓的*层*"局部地"描述. 如果沿着具有同构的局部环的层的开子集把层"黏合"在一起，将得到一个*概形*，概形似乎是研究簇的最好方式. 涉及这一领域的两个最突出的数学家是格罗滕迪克 (A. Grothendieck) 和塞尔(J. -P. Serre).

习题

6.60 证明每个代数闭域都是无限的.

6.61　证明：如果交换环 R 中的元素 a 是幂零的，则 $1+a$ 是单位．

提示：因 a 是幂零的，$1/(1+a)$ 的幂级数经有限项后终止．

6.62　如果 I 是交换环 R 中的理想，证明它的根 $\sqrt{I}$ 是理想．

提示：如果 $f^r \in I$ 和 $g^s \in I$，证明 $(f+g)^{r+s} \in I$．

6.63　如果 R 是交换环，则它的**诣零根** $\mathrm{nil}(R)$ 定义为 R 中一切素理想的交．证明 $\mathrm{nil}(R)$ 是 R 中一切幂零元素的集合：

$$\mathrm{nil}(R)=\{r\in R：有某个\ m\geqslant 1\ 使得\ r^m=0\}.$$

397

提示：如果 $r\in R$ 不是幂零的，用习题 6.9 证明有某个素理想不包含 r.

6.64　(i) 证明 x^2+y^2 在 $\mathbb{R}[x,y]$ 中是不可约的，由此推出 (x^2+y^2) 是 $\mathbb{R}[x,y]$ 中的素理想，并因此是根理想．

(ii) 证明 $\mathrm{Var}(x^2+y^2)=\{(0,0)\}$.

(iii) 证明 $\mathrm{Id}(\mathrm{Var}(x^2+y^2))\supsetneqq(x^2+y^2)$，由此推出 $\mathbb{R}[x,y]$ 中的根理想 (x^2+y^2) 不是某个簇 V 的 $\mathrm{Id}(V)$．并推出，如果 k 不是代数闭的，则零点定理在 $k[x]$ 中可能不成立.

(iv) 证明在 $\mathbb{C}[x,y]$ 中 $(x^2+y^2)=(x+\mathrm{i}y)\cap(x-\mathrm{i}y)$.

(v) 证明在 $\mathbb{C}[x,y]$ 中 $\mathrm{Id}(\mathrm{Var}(x^2+y^2))=(x^2+y^2)$．

6.65　证明：如果 k 是（不可数）代数闭域且 $f_1,\cdots,f_t\in k[X]$，则 $\mathrm{Var}(f_1,\cdots,f_t)=\varnothing$ 当且仅当存在 $h_1,\cdots,h_t\in k[X]$ 使得

$$1=\sum_{i=1}^{t}h_i(X)f_i(X).$$

6.66　设 k 是（不可数）代数闭域，并设 $I=(f_1,\cdots,f_t)\subseteq k[X]$．如果 $g(X)\in k[X]$，证明 $g\in\sqrt{I}\subseteq k[X]$ 当且仅当 $(f_1,\cdots,f_t,1-yg)$ 不是 $k[x,y]$ 中的真理想．

提示：用 Rabinowitch 技巧．

6.67　设 R 是交换环，用 $\mathrm{Spec}(R)$ 表示 R 中一切素理想的集合．如果 I 是 R 中的理想，定义

$$\overline{I}=\{R\ 中一切包含\ I\ 的素理想\}.$$

证明：

(i) $\overline{\{0\}}=\mathrm{Spec}(R)$．

(ii) $\overline{R}=\varnothing$．

(iii) $\overline{\sum_\ell I_\ell}=\bigcap_\ell \overline{I_\ell}$．

(iv) $\overline{I\cap J}=\overline{IJ}=\overline{I}\cup\overline{J}$.

由此推出 $\mathrm{Spec}(R)$ 是一个拓扑空间，它的闭子集是**扎里斯基闭集**：形如 $\overline{I}$ 的那些集合，其中 I 在 R 中的理想上变动．

6.68　证明 $\mathrm{Spec}(R)$ 中的一个理想 P 是闭的（即单点集 $\{P\}$ 是扎里斯基闭集）当且仅当 P 是极大理想．

6.69　假定 X 和 Y 是拓扑空间，则函数 $g:X\to Y$ 称为**连续的**，如果对 Y 的每个闭集 Q，逆象 $g^{-1}(Q)$ 是 X 的闭集．

设 $f:R\to A$ 是环同态，定义 $f^*:\mathrm{Spec}(A)\to\mathrm{Spec}(R)$ 为 $f^*(Q)=f^{-1}(Q)$，其中 Q 是 A 中的素理想．证明 f^* 是连续函数．[回忆根据习题 6.5，$f^{-1}(Q)$ 是素理想．]

6.70　证明由 $\varphi:(a_1,\cdots,a_n)\mapsto(x_1-a_1,\cdots,x_n-a_n)$ 定义的函数 $\varphi:k^n\to\mathrm{Spec}(k[x_1,\cdots,x_n])$ [其中 k 是（不可数）代数闭域] 是一个连续单射（其中 k^n 和 $\mathrm{Spec}(k[x_1,\cdots,x_n])$ 都配置扎里斯基拓扑，k^n 上的扎里斯基拓扑的定义在紧接命题 6.93 的后面）．

398

6.71　证明 k^n 中的闭集的任一降链

$$F_1 \supseteq F_2 \supseteq \cdots \supseteq F_m \supseteq F_{m+1} \supseteq \cdots$$

必有终止，存在某个 t 使得 $F_t = F_{t+1} = \cdots$.

6.72 如果 R 是交换诺特环，证明 R 中的理想 I 是根理想当且仅当 $I = P_1 \cap \cdots \cap P_r$，其中 P_i 是素理想.

6.73 证明在交换环 R 中存在这样的理想 I，I 不是准素的，而$\sqrt{I}$是素的.

提示：取 $R = k[x,y]$，其中 k 是域，$I = (x^2, xy)$.

6.74 设 $R = k[x,y]$，其中 k 是域，并设 $I = (x^2, y)$. 对每个 $a \in k$，证明 $I = (x) \cap (y+ax, x^2)$ 是一个无赘准素分解. 由此推出在一个理想的无赘准素分解中的准素理想未必唯一.

6.6 格罗布纳基

人们误认为传统希腊哲学家轻实验重理性. 例如，他们不去看一个人的嘴数数他的牙，而宁愿猜测多少颗牙齿是一个人所必需的，并由此断定每个人应该有比如 28 颗牙齿. 新兴数学家也喜欢纯理性，但他们也要数牙齿. 如果没有其他理由妨碍我们处理赖以猜测定理的数据，那么计算和算法是有用的. 依此，考虑求一个簇 $\mathrm{Var}(I)$ 的不可约分量的问题；从代数来说，这个问题就是求 I 的相伴素理想. 准素分解定理说，我们应该寻找包含 I 的准素理想 Q_i，而所求的分量就是 $\mathrm{Var}(\sqrt{Q_i})$. 然而在定理 6.116 的证明中，我们看到如果 $I = Q_1 \cap \cdots \cap Q_r$ 是无赘准素分解，其中 Q_i 是 P_i-准素的，则 $P_i = \sqrt{(I : c_i)}$，其中 $c_i \in \bigcap_{j \neq i} Q_j$ 且 $c \notin Q_i$. 老老实实地观察牙齿涉及下面的问题. 给定 I 的生成元的集合，我们能够确切地求出 P_i 的生成元吗? 困难在于寻求元素 c_i，在本节中将表明如何寻求 $\sqrt{(I : c)}$ 的生成元. 除了这一点之外，我们还必须说算法不仅在特别情形中提供数据，它的作用比这更多. 例如，对于域扩张 K/k，如果 $f(x), g(x) \in k[x]$，则它们在 $K[x]$ 中的 gcd 等于它们在 $k[x]$ 中的 gcd，其证明方法本质上是运用了欧几里得算法.

给定两个多项式 $f(x), g(x) \in k[x]$，其中 $g(x) \neq 0$，k 是域，什么时候 $g(x)$ 是 $f(x)$ 的因式? 带余除法给出唯一的多项式 $q(x), r(x) \in k[x]$ 使得

$$f(x) = q(x)g(x) + r(x),$$

其中 $r = 0$ 或 $\deg(r) < \deg(g)$，而 $g \mid f$ 当且仅当余式 $r = 0$. 我们从另一种不同的观点来看这个公式. 说 $g \mid f$ 就是说 $f \in (g)$，(g) 是 $g(x)$ 生成的主理想. 这样，余式 r 是 f 进入这个理想的障碍，即 $f \in (g)$ 当且仅当 $r = 0$.

399

考虑更一般的问题. 给定多项式

$$f(x), g_1(x), \cdots, g_m(x) \in k[x],$$

其中 k 是域，什么时候 $d(x) = \gcd\{g_1(x), \cdots, g_m(x)\}$ 是 f 的因式? 欧几里得算法可求出 d，而带余除法确定是否 $d \mid f$. 从另一个观点来看，两个经典算法联合起来给出判定是否有 $f \in (g_1, \cdots, g_m) = (d)$ 的算法.

我们现在要问在 $k[x_1, \cdots, x_n] = k[X]$ 中是否存在一个算法对给定的 $f(X), g_1,(X), \cdots, g_m(X) \in k[X]$ 可以判定是否有 $f \in (g_1, \cdots, g_m)$. $k[X]$ 中的一个广义带余除法应该是这样的算法，它产生

$$r(X), a_1(X), \cdots, a_m(X) \in k[X],$$

其中 $r(X)$ 是唯一的，使得

$$f = a_1 g_1 + \cdots + a_m g_m + r$$

且 $f \in (g_1, \cdots, g_m)$ 当且仅当 $r = 0$. 因 $(g_1, \cdots, g_m)$ 由各个 g 的一切线性组合构成，这样的算法说余式 r 是 f 进入 $(g_1, \cdots, g_m)$ 的障碍.

我们要证明带余除法和欧几里得算法都可以扩展到多元多项式上．虽然这些结果是初等的，但是直到最近的 1965 年才被 B. Buchberger 发现．代数常处理算法，但 19 世纪下半叶自凯莱和戴德金之后，公理化方法的能力和精妙使它占据着优势．随着 1948 年晶体管的发明，高速计算成为现实，老的复杂算法和新的算法都可以被实现，高阶计算进入了代数．计算机科学的发展极可能是把一元多项式的经典算法推广到多元多项式为什么直到现在才被发现的根本原因．这生动地说明了数学外部思想的影响力．

6.6.1 广义带余除法

$k[x]$ 中带余除法的最重要的特征是余式 $r(x)$ 有较小次数．没有不等式 $\deg(r)<\deg(g)$，这个结果实质上是无用的，毕竟，给定任一 $Q(X)\in k[x]$，有等式

$$f(x)=Q(x)g(x)+[f(x)-Q(x)g(x)].$$

现在多元多项式是单项式 $cx_1^{\alpha_1}\cdots x_n^{\alpha_n}$ 的和，其中 $c\in k$ 且对一切 i 有 $\alpha_i\geqslant 0$．有两种次数可以指派给单项式．

400

定义 一个单项式 $cx_1^{\alpha_1}\cdots x_n^{\alpha_n}\in k[x_1,\cdots,x_n]$ 的**多元次数**是 n 元组 $\alpha=(\alpha_1,\cdots,\alpha_n)$，其中 $c\in k$ 是非零的且对一切 $i,\alpha_i\geqslant 0$．它的**权**是和 $|\alpha|=\alpha_1+\cdots+\alpha_n$.

在 $k[x]$ 中用 $g(x)$ 除 $f(x)$ 的时候，我们常把 $f(x)$ 中的单项式按照次数排成降序：

$$f(x)=c_nx^n+c_{n-1}x^{n-1}+\cdots+c_2x^2+c_1x+c_0.$$

如果把 $(\alpha_1,\cdots,\alpha_n)$ 缩写为 α，把 $x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ 缩写为 X^α，则多元多项式

$$f(X)=f(x_1,\cdots,x_n)=\sum c_{(\alpha_1,\cdots,\alpha_n)}x_1^{\alpha_1}\cdots x_n^{\alpha_n}$$

可简写为

$$f(X)=\sum_\alpha c_\alpha X^\alpha.$$

我们将对单项式的多元次数进行排序，从而把 $f(X)$ 中的单项式给予合理的排列．

在例5.69(ii)中，我们看到自然数的一切 n 元组的集合$\mathbb{N}^n$ 是在加法下的幺半群：

$$\alpha+\beta=(\alpha_1,\cdots,\alpha_n)+(\beta_1,\cdots,\beta_n)=(\alpha_1+\beta_1,\cdots,\alpha_n+\beta_n).$$

这个幺半群运算与单项式的乘法相关：

$$X^\alpha X^\beta=X^{\alpha+\beta}.$$

回忆偏序集是一个集合 X 配置了自反、反对称和传递的关系$\preceq$. 当然可以把 $x\preceq y$ 且 $x\neq y$ 写为 $x\prec y$，还可以用 $y\succeq x$（或 $y\succ x$）代替 $x\preceq y$（或 $x\prec y$）．一个偏序集 X 是良序的，如果每个非空子集 $S\subseteq X$ 都包含一个最小元素；即存在 $s_0\in S$ 满足对一切 $s\in S$ 有 $s_0\preceq s$．例如，最小整数公理说自然数$\mathbb{N}$ 连同通常的不等性$\leqslant$是良序的．

附录中的命题 A.3 证明在良序集中每个严格递减序列必有限．良序集的这个性质可以用来证明一个算法最终停止．例如，在一元多项式的带余除法的证明中我们让每一步对应一个自然数：余式的次数．此外，如果该算法在给定的步数后不停止，则下一步对应的自然数——余式的次数——严格地变小．因自然数在通常的不等性$\leqslant$下成为良序集，所以这个严格递减的自然数序列必有限，即该算法经有限步后必终止．

我们的兴趣是给多元次数排序，这个序要和单项式的乘法相容——即与幺半群$\mathbb{N}^n$ 中的加法相容．

401

定义 **单项序**是指$\mathbb{N}^n$的良序满足对一切$\alpha,\beta,\gamma\in\mathbb{N}^n$，

$$\alpha\leq\beta \text{ 蕴涵 } \alpha+\gamma\leq\beta+\gamma.$$

单项序可如下运用．如果$X=(x_1,\cdots,x_n)$，则当$\alpha\leq\beta$时我们定义$X^\alpha\leq X^\beta$，即单项式可按照它们的多元次数排序．

定义 如果$\mathbb{N}^n$配置了单项序，则每个$f(X)\in k[X]=k[x_1,\cdots,x_n]$可以把它的最大项写在前面，接着用降序方式写出它的较小的项：

$$f(X)=c_\alpha X^\alpha+\text{低次项}.$$

定义它的**首项**为$\mathrm{LT}(f)=c_\alpha X^\alpha$，它的**次数**为$\mathrm{Deg}(f)=\alpha$．$f(X)$称为**首一的**，如果$\mathrm{LT}(f)=X^\alpha$，即$c_\alpha=1$．

注意$\mathrm{Deg}(f)$和$\mathrm{LT}(f)$依赖于单项序．

有许多单项序的例子，但我们只给出两个最普通的．

定义 $\mathbb{N}^n$上的**字典序**定义为$\alpha\leq_{\mathrm{lex}}\beta$，如果$\alpha=\beta$或$\beta-\alpha$中的第一个非零坐标是正的．[⊖]

术语字典指的是字典中字的标准顺序．例如下面的德语字在字典序中递增（字母排序为$a<b<c<\cdots<z$）：

ausgehen
ausladen
auslagen
auslegen
bedeuten

如果$\alpha<_{\mathrm{lex}}\beta$，则它们最前的$i-1$个坐标一致（对某个$i\geq1$），即$\alpha_1=\beta_1,\cdots,\alpha_{i-1}=\beta_{i-1}$，并存在严格的不等式：$\alpha_i<\beta_i$．

命题 6.121 字典序$\leq_{\mathrm{lex}}$是$\mathbb{N}^n$上的单项序．

证明 首先我们证明字典序是偏序．关系$\leq_{\mathrm{lex}}$是自反的，因为它的定义表明$\alpha\leq_{\mathrm{lex}}\alpha$．为证明反对称，假定$\alpha\leq_{\mathrm{lex}}\beta$和$\beta\leq_{\mathrm{lex}}\alpha$．如果$\alpha\neq\beta$，则存在第一个不一致的坐标，比如第$i$个．为简化记号，可以假定$\alpha_i<\beta_i$．但这与$\beta\leq_{\mathrm{lex}}\alpha$矛盾．为证明传递性，假设$\alpha<_{\mathrm{lex}}\beta$和$\beta<_{\mathrm{lex}}\gamma$（只要考虑严格不等式就够了）．现在$\alpha_1=\beta_1,\cdots,\alpha_{i-1}=\beta_{i-1}$和$\alpha_i<\beta_i$．设$\gamma_p$是第一个满足$\beta_p<\gamma_p$的坐标．如果$p<i$，则

402

$$\gamma_1=\beta_1=\alpha_1,\cdots,\gamma_{p-1}=\beta_{p-1}=\alpha_{p-1},\alpha_p=\beta_p<\gamma_p;$$

如果$p\geq i$，则

$$\gamma_1=\beta_1=\alpha_1,\cdots,\gamma_{i-1}=\beta_{i-1}=\alpha_{i-1},\alpha_i<\beta_i=\gamma_i.$$

在两种情形中，$\gamma-\alpha$的第一个非零坐标都是正的，即$\alpha<_{\mathrm{lex}}\gamma$．

其次，我们证明字典序是良序．如果S是$\mathbb{N}^n$的非空子集，定义

$$C_1=\{S\text{ 中一切 }n\text{ 元组的第一个坐标}\},$$

并定义δ_1为C_1中的最小数（注意C_1是良序集$\mathbb{N}$的非空子集）．定义

$$C_2=\{\text{一切 }n\text{ 元组}(\delta_1,\alpha_2,\cdots,\alpha_n)\in S\text{ 的第二个坐标}\}.$$

因$C_2\neq\varnothing$，它包含最小数δ_2．同样，对一切$i<n$定义C_{i+1}为S中最先i个坐标是$(\delta_1,\cdots,\delta_i)$的那些$n$元组的第$i+1$个坐标，并定义$\delta_{i+1}$为$C_{i+1}$中的最小数．根据构造方法，$n$元组$\delta=(\delta_1,\delta_2,\cdots,\delta_n)$

⊖ 差$\beta-\alpha$可能不在$\mathbb{N}^n$中，但它在$\mathbb{Z}^n$中．

在 S 中，此外，如果 $\alpha=(\alpha_1,\alpha_2,\cdots,\alpha_n)\in S$，则

$$\alpha-\delta=(\alpha_1-\delta_1,\alpha_2-\delta_2,\cdots,\alpha_n-\delta_n)$$

的第一个非零坐标如果有的话必是正的，从而 $\delta\prec_{\text{lex}}\alpha$. 所以字典序是良序．

假定 $\alpha\preceq_{\text{lex}}\beta$，我们断言对一切 $\gamma\in\mathbb{N}^n$，

$$\alpha+\gamma\preceq_{\text{lex}}\beta+\gamma.$$

如果 $\alpha=\beta$，则 $\alpha+\gamma=\beta+\gamma$. 如果 $\alpha\prec_{\text{lex}}\beta$，则 $\beta-\alpha$ 的第一个非零坐标是正的．但

$$(\beta+\gamma)-(\alpha+\gamma)=\beta-\alpha,$$

从而 $\alpha+\gamma\prec_{\text{lex}}\beta+\gamma$. 所以 $\preceq_{\text{lex}}$ 是单项序． ■

在字典序中，$x_1>x_2>x_3>\cdots$，因为

$$(1,0,\cdots,0)\succ(0,1,0,\cdots,0)\succ\cdots\succ(0,0,\cdots,1).$$

变量 $x_{\sigma(1)},\cdots,x_{\sigma(n)}$ 的任何一个置换产生 $\mathbb{N}^n$ 中不同的字典序． [403]

注 如果 X 是具有序 $\preceq$ 的任一良序集，则 X^n 上的字典序可以定义为 $a=(a_1,\cdots,a_n)\preceq_{\text{lex}}b=(b_1,\cdots,b_n)$，如果 $a=b$ 或它们第一个不一致的坐标是第 i 个坐标且 $a_i\prec b_i$. 用 X 替换 $\mathbb{N}$ 以推广命题 6.121 是一件简单的事． ■

在引理 5.70 中，我们对任意集合 X 构造了幺半群 $\mathcal{W}(X)$，它的元素是空字以及集合 X 上的一切字 $x_1^{e_1}\cdots x_p^{e_p}$，其中 $p\geqslant 1$ 且对一切 i, $e_i=\pm 1$，它的运算是并置．和 $\mathbb{N}^n$ 相比，$\mathbb{N}^n$ 中一切字的长度都是 n，而幺半群 $\mathcal{W}(X)$ 有不同长度的字．当然这里更重要的是 $\mathcal{W}(X)$ 的子幺半群 $\mathcal{W}^+(X)$，它由 X 上的一切"正"字组成：

$$\mathcal{W}^+(X)=\{x_1\cdots x_p\in\mathcal{W}(X):x_i\in X\text{ 且 }p\geqslant 0\}.$$

系 6.122 如果 X 是良序集，则 $\mathcal{W}^+(X)$ 在字典序（也记为 $\preceq_{\text{lex}}$）中是良序集．

证明 我们这里只给出字典序的谨慎的定义，而把它是良序集的证明留给读者．首先，对一切 $w\in\mathcal{W}^+(X)$ 定义 $1\preceq_{\text{lex}}w$. 其次，给定 $\mathcal{W}^+(X)$ 中的字 $u=x_1\cdots x_p$ 和 $v=y_1\cdots y_q$，在较短字的后端添加若干 1 使得它们长度相等，并把它们重新命名为 $\mathcal{W}^+(X)$ 中的 u' 和 v'. 如果 $m\geqslant\max\{p,q\}$，则可以认为 $u',v'\in X^m$，而如果在 X^m 中 $u'\preceq_{\text{lex}}v'$，则定义 $u\preceq_{\text{lex}}v$.（这是字典中通常使用的字的顺序，其中空格排在任一字母的前面，例如 muse 排在 museum 的前面．） ■

引理 6.123 给定 $\mathbb{N}^n$ 上的单项序，任何形如 $f(X)\to f(X)-c_\beta X^\beta+g(X)$ 的变换序列的步数必有限，其中 $c_\beta X^\beta$ 是 $f(X)$ 中的非零项，且 $\text{Deg}(g)\prec\beta$.

证明 每个多项式

$$f(X)=\sum_\alpha c_\alpha X^\alpha\in k[X]=k[x_1,\cdots,x_n]$$

都可以按照项的多元次数按递减序写出：$\alpha_1\succ\alpha_2\succ\cdots\succ\alpha_p$．定义

$$\text{多元字}(f)=\alpha_1\cdots\alpha_p\in\mathcal{W}^+(\mathbb{N}^n).$$

设 $c_\beta X^\beta$ 是 $f(X)$ 中的非零项，并设 $g(X)\in k[X]$ 有 $\text{Deg}(g)\prec\beta$，记

$$f(X)=h(X)+c_\beta X^\beta+\ell(X),$$

其中 $h(X)$ 是 $f(X)$ 中多元次数 $\succ\beta$ 的那些项的和，而 $\ell(X)$ 是 $f(X)$ 中多元次数 $\prec\beta$ 的那些项的和．我们断言在 $\mathcal{W}^+(X)$ 中

$$\begin{aligned}\text{多元字}(f(X)-c_\beta X^\beta+g(X))&\preceq_{\text{lex}}\text{多元字}(h+\ell+g)\\&\prec_{\text{lex}}\text{多元字}(f).\end{aligned}$$

[404]

$f(X)-c_\beta X^\beta+g(X)$中多元次数$>\beta$的那些项的和是$h(X)$，而较小的那些项的和是$\ell(X)+g(X)$。但由习题6.79，$\mathrm{Deg}(\ell+g)\prec\beta$. 所以$f(X)$和$f(X)-c_\beta X^\beta+g(X)$中的初始项相同，而$f(X)-c_\beta X^\beta+g(X)$中的下一项的多元次数$\prec\beta$，由此证明了我们的断言．因$\mathcal{W}^+(\mathbb{N}^n)$是良序集，因此形如$f(X)\to f(X)-c_\beta X^\beta+g(X)$的变换序列的步数必有限． ■

下面是第二种普通的单项序．回忆如果$\alpha=(\alpha_1,\cdots,\alpha_n)\in\mathbb{N}^n$，则$|\alpha|=\alpha_1+\cdots+\alpha_n$表示它的权．

定义 $\mathbb{N}^n$上的**次数-字典序**定义为$\alpha\preceq_{\mathrm{dlex}}\beta$，如果$\alpha=\beta$或

$$|\alpha|=\sum_{i=1}^n\alpha_i<\sum_{i=1}^n\beta_i=|\beta|,$$

或$|\alpha|=|\beta|$，而$\beta-\alpha$中的第一个非零坐标是正的．

换句话说，给定$\alpha=(\alpha_1,\cdots,\alpha_n)$和$\beta=(\beta_1,\cdots,\beta_n)$，先检查权，如果$|\alpha|<|\beta|$，则$\alpha\preceq_{\mathrm{dlex}}\beta$，如果是平局，即$\alpha$和$\beta$的权相等，则用字典序排序．例如$(1,2,3,0)\prec_{\mathrm{dlex}}(0,2,5,0)$和$(1,2,3,4)\prec_{\mathrm{dlex}}(1,2,5,2)$.

命题6.124 次数-字典序$\preceq_{\mathrm{dlex}}$是$\mathbb{N}^n$上的单项序．

证明 容易验证$\preceq_{\mathrm{dlex}}$是$\mathbb{N}^n$上的偏序．为证它是良序，设S是$\mathbb{N}^n$的非空子集．S中元素的权形成$\mathbb{N}$的非空子集，从而有最小的一个，比如t. 有权t的一切$\alpha\in S$形成的非空子集有最小元素，这是因为在这个子集上，次数-字典序$\preceq_{\mathrm{dlex}}$和字典序$\preceq_{\mathrm{lex}}$一致．所以在S中关于次数-字典序有最小元素．

假定$\alpha\preceq_{\mathrm{dlex}}\beta$和$\gamma\in\mathbb{N}^n$. 现在$|\alpha+\gamma|=|\alpha|+|\gamma|$，从而$|\alpha|=|\beta|$蕴涵$|\alpha+\gamma|=|\beta+\gamma|$，且$|\alpha|<|\beta|$蕴涵$|\alpha+\gamma|<|\beta+\gamma|$；对于后一种情形，命题6.121表明$\alpha+\gamma\preceq_{\mathrm{dlex}}\beta+\gamma$. ■

下一命题表明，关于单项序，多元多项式的表现和一元多项式相似．

命题6.125 设$\preceq$是$\mathbb{N}^n$上的单项序，并设$f(X),g(X),h(X)\in k[X]=k[x_1,\cdots,x_n]$，其中$k$是域．

(i) 如果$\mathrm{Deg}(f)=\mathrm{Deg}(g)$，则$\mathrm{LT}(g)\mid\mathrm{LT}(f)$.

(ii) $\mathrm{LT}(hg)=\mathrm{LT}(h)\,\mathrm{LT}(g)$.

405

(iii) 如果$\mathrm{Deg}(f)=\mathrm{Deg}(hg)$，则$\mathrm{LT}(g)\mid\mathrm{LT}(f)$.

证明 (i) 如果$\mathrm{Deg}(f)=\alpha=\mathrm{Deg}(g)$，则$\mathrm{LT}(f)=cX^\alpha$和$\mathrm{LT}(g)=dX^\alpha$. 因$c\neq0$，从而$c$是$k$中的单位，所以$\mathrm{LT}(g)\mid\mathrm{LT}(f)$[注意，也有$\mathrm{LT}(f)\mid\mathrm{LT}(g)$].

(ii) 设$h(X)=cX^\gamma+$低次项，$g(X)=bX^\beta+$低次项，从而$\mathrm{LT}(h)=cX^\gamma$，$\mathrm{LT}(g)=bX^\beta$. 显然，$cbX^{\gamma+\beta}$是$h(X)g(X)$的非零项．为证明它是首项，设$c_\mu X^\mu$是$h(X)$的一项满足$\mu\preceq\gamma$，$b_\nu X^\nu$是$g(X)$的一项满足$\nu\preceq\beta$(其中至少一个有严格不等性)．现在$\mathrm{Deg}(c_\mu X^\mu b_\nu X^\nu)=\mu+\nu$，因$\preceq$是单项序，我们有$\mu+\nu\prec\gamma+\nu\prec\gamma+\beta$，因此$cbX^{\gamma+\beta}$是$h(X)g(X)$中具有最大多元次数的项．

(iii) 因$\mathrm{Deg}(f)=\mathrm{Deg}(hg)$，(i) 给出$\mathrm{LT}(hg)\mid\mathrm{LT}(f)$，根据(ii)，$\mathrm{LT}(h)\,\mathrm{LT}(g)=\mathrm{LT}(hg)$，因此$\mathrm{LT}(g)\mid\mathrm{LT}(f)$. ■

定义 设$\preceq$是$\mathbb{N}^n$上的单项序，并设$f(X),g(X)\in k[X]$，其中$k[X]=k[x_1,\cdots,x_n]$. 如果在$f(X)$中有非零项$c_\beta X^\beta$满足$\mathrm{LT}(g)\mid c_\beta X^\beta$和

$$h(X)=f(X)-\frac{c_\beta X^\beta}{\mathrm{LT}(g)}g(X),$$

则**约化**$f\xrightarrow{g}h$是指用h替换f.

约化正好是一元多项式的长除法中通常包含的步骤．当然，约化的一个特殊情形是$c_\beta X^\beta=$

LT (f).

命题 6.126 设$\preceq$是$\mathbb{N}^n$上的单项序，并设 $f(X), g(X) \in k[X] = k[x_1, \cdots, x_n]$，假定 $f \xrightarrow{g} h$，即有 $f(X)$ 的非零项 $c_\beta X^\beta$ 满足 $\mathrm{LT}(g) \mid c_\beta X^\beta$ 和 $h(X) = f(X) - \frac{c_\beta X^\beta}{\mathrm{LT}(g)} g(X)$. 则

$$\mathrm{Deg}\left(\frac{c_\beta X^\beta}{\mathrm{LT}(g)} g(X)\right) \preceq \mathrm{Deg}(f).$$

此外，如果 $\beta = \mathrm{Deg}(f)$ [即如果 $c_\beta X^\beta = \mathrm{LT}(f)$]，则

$$h(X) = 0 \text{ 或 } \mathrm{Deg}(h) \prec \mathrm{Deg}(f).$$

如果 $\beta \prec \mathrm{Deg}(f)$，则 $\mathrm{Deg}(h) = \mathrm{Deg}(f)$.

证明 记

$$f(X) = \mathrm{LT}(f) + c_\kappa X^\kappa + \text{低次项},$$

其中 $c_\kappa X^\kappa = \mathrm{LT}(f - \mathrm{LT}(f))$. 因 $c_\beta X^\beta$ 是 $f(X)$ 的一项，所以有 $\beta \preceq \mathrm{Deg}(f)$. 同样，如果 $\mathrm{LT}(g) = a_\gamma X^\gamma$，则 $\mathrm{Deg}(g) = \gamma$，记

$$g(X) = a_\gamma X^\gamma + a_\lambda X^\lambda + \text{低次项},$$

406

其中 $a_\lambda X^\lambda = \mathrm{LT}(g - \mathrm{LT}(g))$. 因此

$$\begin{aligned} h(X) &= f(X) - \frac{c_\beta X^\beta}{\mathrm{LT}(g)} g(X) \\ &= f(X) - \frac{c_\beta X_\beta}{\mathrm{LT}(g)} [\mathrm{LT}(g) + a_\lambda X^\lambda + \cdots] \\ &= [f(X) - c_\beta X^\beta] - \frac{c_\beta X^\beta}{\mathrm{LT}(g)} [a_\lambda X^\lambda + \cdots]. \end{aligned}$$

现在 $\mathrm{LT}(g) \mid c_\beta X^\beta$ 说明 $\beta - \gamma \in \mathbb{N}^n$. 我们断言

$$\mathrm{Deg}\left(-\frac{c_\beta X^\beta}{\mathrm{LT}(g)} [a_\lambda X^\lambda + \cdots]\right) = \lambda + \beta - \gamma;$$

即 $\lambda + \beta - \gamma = \mathrm{Deg}\left(-\frac{c_\beta X^\beta}{\mathrm{LT}(g)} a_\lambda X^\lambda\right)$是出现的最大多元次数. 假设 $a_\eta X^\eta$ 是 $g(X)$ 中的低次项（即 $\eta \prec \lambda$）；因$\preceq$是单项序，有

$$\eta + (\beta - \gamma) \prec \gamma + (\lambda - \gamma) = \lambda.$$

现在 $\lambda \prec \gamma$ 蕴涵 $\lambda + (\beta - \gamma) \prec \gamma + (\beta - \gamma) = \beta$，从而

$$\mathrm{Deg}\left(-\left[\frac{c_\beta X^\beta}{\mathrm{LT}(g)}\right] g(X)\right) \prec \beta \preceq \mathrm{Deg}(f). \tag{6}$$

所以，如果 $h(X) \neq 0$，则习题 6.79 给出

$$\mathrm{Deg}(h) \preceq \max\left\{\mathrm{Deg}(f(X) - c_\beta X^\beta), \mathrm{Deg}\left(-\left[\frac{c_\beta X^\beta}{\mathrm{LT}(g)}\right] g(X)\right)\right\}.$$

现在如果 $\beta = \mathrm{Deg}(f)$，则 $c_\beta X^\beta = \mathrm{LT}(f)$，

$$f(X) - c_\beta X^\beta = f(X) - \mathrm{LT}(f) = c_\kappa X^\kappa + \text{低次项},$$

因此在这种情形中 $\mathrm{Deg}(f(X) - c_\beta X^\beta) = \kappa \prec \mathrm{Deg}(f)$. 如果 $\beta \prec \mathrm{Deg}(f)$，则 $\mathrm{Deg}(f(X) - c_\beta X^\beta) = \mathrm{Deg}(f)$，而根据(6)式，$\mathrm{Deg}\left(-\left[\frac{c_\beta X^\beta}{\mathrm{LT}(g)}\right] g(X)\right) \prec \mathrm{Deg}(f)$，从而在这种情形中 $\mathrm{Deg}(h) = \mathrm{Deg}(f)$.

最后一个不等式是明显的，因为

$$\frac{c_\beta X^\beta}{\mathrm{LT}(g)}g(X)=c_\beta X^\beta+\frac{c_\beta X^\beta}{\mathrm{LT}(g)}[a_\lambda X^\lambda+\cdots].$$

因多项式后面部分的多元次数为 $\lambda+\beta-\gamma<\beta$，由此可知

407

$$\mathrm{Deg}\left(\frac{c_\beta X^\beta}{\mathrm{LT}(g)}g(X)\right)=\beta\preceq\mathrm{Deg}(f).$$

■

定义 设 $\{g_1(X),\cdots,g_m(X)\}$ 是 $k[X]$ 中多项式的集合．多项式 $r(X)$ 称为 $\mathrm{mod}\{g_1,\cdots,g_m\}$ **约化的**，如果 $r(X)=0$ 或没有一个 $\mathrm{LT}(g_i)$ 整除 $r(X)$ 的任一非零项．

下面是多元多项式的带余除法．因为算法要求在特殊的序中运用"因式多项式"$\{g_1,\cdots,g_m\}$（毕竟一个算法必须给出确切的方向），我们将用多项式的 m 元组替代多项式的子集．记第 i 个元素是 g_i 的 m 元组为 $[g_1,\cdots,g_m]$，因为常用的记号 $(g_1,\cdots,g_m)$ 会和 g_i 生成的理想 $(g_1,\cdots,g_m)$ 产生混淆．

定理 6.127（$k[X]$中的带余除法） 设 $\preceq$ 是 $\mathbb{N}^n$ 上的单项序，$k[X]=k[x_1,\cdots,x_n]$．如果 $f(X)\in k[X]$ 和 $G=[g_1(X),\cdots,g_m(X)]$ 是 $k[X]$ 中多项式的 m 元组，则存在一个算法给出多项式 $r(X),a_1(X),\cdots,a_m(X)\in k[X]$ 使得

$$f=a_1g_1+\cdots+a_mg_m+r,$$

其中 r 是 $\mathrm{mod}\{g_1,\cdots,g_m\}$ 约化的，且

$$\text{对一切 } i\text{，}\mathrm{Deg}(a_ig_i)\preceq\mathrm{Deg}(f).$$

证明 单项序一旦选定，首项就有定义，该算法是一元多项式的带余除法的直接推广．首先，用 $\mathrm{mod}\,g_1$ 约化尽可能多次，然后用 $\mathrm{mod}\,g_2$ 约化尽可能多次，再用 $\mathrm{mod}\,g_1$ 约化；一般地，一旦多项式对任意 i 被 $\mathrm{mod}[g_1,\cdots,g_i]$ 约化，则用 $\mathrm{mod}[g_1,\cdots,g_i,g_{i+1}]$ 约化．下面的伪码更精确地描述了这个算法．

Input: $f(X)=\sum_\beta c_\beta X^\beta,[g_1,\cdots,g_m]$

Output: $r,a_1,\cdots,a_m$

$r:=f;a_i:=0$

WHILE f is not reduced $\mathrm{mod}\{g_1,\cdots,g_m\}$ DO

  select smallest i with $\mathrm{LT}(g_i)\mid c_\beta X^\beta$ for β maximal such that

  $f-[c_\beta X^\beta/\mathrm{LT}(g_i)]g_i:=f$

  $a_i+[c_\beta X^\beta/\mathrm{LT}(g_i)]:=a_i$

END WHILE

对于这个算法的每一步 $h_j\xrightarrow{g_i}h_{j+1}$，根据引理 6.123，在$\mathcal{W}^+(\mathbb{N}^n)$ 中有

$$\text{多元字}(h_j)\succ_{\mathrm{lex}}\text{多元字}(h_{j+1}),$$

因$\prec_{\mathrm{lex}}$是$\mathcal{W}^+(\mathbb{N}^n)$上的良序，所以该算法必终止．显然最终输出的 $r(X)$ 是 $\mathrm{mod}\{g_1,\cdots,g_m\}$ 约化的，这是因为 $r(X)$ 某一项如果被某个 $\mathrm{LT}(g_i)$ 整除，则可以进一步约化．

最后，对某个中间输出 $h(X)$，$a_i(X)$ 的每个项形如 $c_\beta X^\beta/\mathrm{LT}(g_i)$（如同在伪码中所见）．现在

408

根据命题 6.126，$\mathrm{Deg}(a_ig_i)\preceq\mathrm{Deg}(f)$． ■

定义 给定$\mathbb{N}^n$上的单项序，多项式 $f(X)\in k[X]$ 和 m 元组 $G=[g_1,\cdots,g_m]$，带余除法的输出 $r(X)$ 称为 $f(X)\,\mathrm{mod}\,G$ **的余式**．

注意 $f \bmod G$ 的余式 r 是 $\bmod \{g_1,\cdots,g_m\}$ 约化的且 $f-r \in I=(g_1,\cdots,g_m)$．该算法要求 G 是 m 元组，因为命令

$$\text{选取最小的 } i \text{ 使得对某个 } \beta \text{ 有 } \mathrm{LT}(g_i) \mid c_\beta X^\beta$$

指定了约化的次序．

下一个例子说明余式不仅依赖于多项式集合 $\{g_1,\cdots,g_m\}$，也依赖于 m 元组 $G=[g_1,\cdots,g_m]$ 中坐标的排序．即如果 $\sigma \in S_m$ 是置换且 $G_\sigma=[g_{\sigma(1)},\cdots,g_{\sigma(m)}]$，则 $f \bmod G_\sigma$ 的余式 r_σ 可能和 $f \bmod G$ 的余式 r 不同．更坏的是有可能 $r \neq 0$ 而 $r_\sigma=0$，从而 $\bmod G$ 的余式不是 f 进入理想 $(g_1,\cdots,g_m)$ 的障碍．我们在下一例中解释这个现象，并在下一小节中处理它．

例 6.128 设 $f(x,y,z)=x^2y^2+xy$，并设 $G=[g_1,g_2,g_3]$，其中

$$g_1=y^2+z^2$$
$$g_2=x^2y+yz$$
$$g_3=z^3+xy.$$

我们用$\mathbb{N}^3$ 中的次数-字典序．现在 $y^2=\mathrm{LT}(g_1) \mid \mathrm{LT}(f)=x^2y^2$，从而 $f \xrightarrow{g_1} h$，其中

$$h=f-\frac{x^2y^2}{y^2}(y^2+z^2)=-x^2z^2+xy.$$

多项式 $-x^2z^2+xy$ 是 $\bmod G$ 约化的，因为不管是 $-x^2z^2$ 还是 xy 都不能被任意一个首项 $\mathrm{LT}(g_1)=y^2$，$\mathrm{LT}(g_2)=x^2y$ 或 $\mathrm{LT}(g_3)=z^3$ 整除．

现在用 3 元组 $G'=[g_2,g_1,g_3]$ 做带余除法．第一次约化给出 $f \xrightarrow{g_2} h'$，其中

$$h'=f-\frac{x^2y^2}{x^2y}(x^2y+yz)=-y^2z+xy.$$

现在 h' 不是约化的，$\bmod g_1$ 约化给出

$$h'-\frac{-y^2z}{y^2}(y^2+z^2)=z^3+xy.$$

但 $z^3+xy=g_3$，所以 $z^3+xy \xrightarrow{g_3} 0$．因此，余式依赖于 m 元组中因式多项式 g_i 的排序．

余式不同的更简单的例子（但没有余式为 0）见习题 6.78． ■ [409]

习题

6.75 （i）设 $(X,\preceq)$ 和$(Y,\preceq')$ 是良序集，其中 X 和 Y 不相交．定义 $X \cup Y$ 上的二元关系$\leqslant$为

$$x_1 \leqslant x_2 \quad \text{如果 } x_1,x_2 \in X \text{ 且 } x_1 \preceq x_2,$$
$$y_1 \leqslant y_2 \quad \text{如果 } y_1,y_2 \in Y \text{ 且 } y_1 \preceq' y_2,$$
$$x \leqslant y \quad \text{如果 } x \in X \text{ 和 } y \in Y.$$

证明 $(X \cup Y,\leqslant)$ 是良序集．

（ii）如果 $r \leqslant n$，则可以把$\mathbb{N}^r$ 看作由形如 $(n_1,\cdots,n_r,0,\cdots,0)$ 的一切 n 元组组成的$\mathbb{N}^n$ 的子集，其中对一切 $i \leqslant r$，$n_i \in \mathbb{N}$. 证明存在$\mathbb{N}^n$ 上的单项序满足当 $\alpha \in \mathbb{N}^r$ 和 $\beta \in \mathbb{N}^n-\mathbb{N}^r$ 时有 $\alpha \prec \beta$.

提示：考虑 $k[x_1,\cdots,x_n]$ 上的字典序，其中 $x_1 \prec x_2 \prec \cdots \prec x_n$．

6.76 （i）用字典序和次数-字典序写出 $k[x,y]$ 中前 10 个首一单项式．

（ii）用字典序和次数-字典序写出 $k[x,y,z]$ 中权最多为 2 的一切首一单项式．

6.77 举出良序集 X 的例子，它包含一个具有无限多个前导的元素 u，即 $\{x \in X : x \preceq u\}$ 是无限集．

6.78 设 $G = [x-y, x-z]$ 和 $G' = [x-z, x-y]$．证明（在次数-字典序中）$x \bmod G$ 的余式和 $x \bmod G'$ 的余式不同．

6.79 设 $\preceq$ 是 $\mathbb{N}^n$ 上的单项序，并设 $f(X), g(X) \in k[X] = k[x_1, \cdots, x_n]$ 是非零多项式．

（i）证明：如果 $f+g \neq 0$，则 $\mathrm{Deg}(f+g) \preceq \max\{\mathrm{Deg}(f), \mathrm{Deg}(g)\}$，且严格不等式只有当 $\mathrm{Deg}(f) = \mathrm{Deg}(g)$ 时才可能产生．

（ii）证明 $\mathrm{Deg}(fg) = \mathrm{Deg}(f) + \mathrm{Deg}(g)$，且对一切 $m \geqslant 1$，$\mathrm{Deg}(f^m) = m\mathrm{Deg}(f)$．

6.80 在本题中用次数-字典序．

（i）求 $x^7y^2 + x^3y^2 - y + 1 \bmod [xy^2 - x, x - y^3]$ 的余式．

（ii）求 $x^7y^2 + x^3y^2 - y + 1 \bmod [x - y^3, xy^2 - x]$ 的余式．

6.81 在本题中用次数-字典序．

（i）求 $x^2y + xy^2 + y^2 \bmod [y^2 - 1, xy - 1]$ 的余式．

（ii）求 $x^2y + xy^2 + y^2 \bmod [xy - 1, y^2 - 1]$ 的余式．

6.82 设 $c_\alpha X^\alpha$ 是非零单项式，并设 $f(X), g(X) \in k[X]$ 是每个项都不被 $c_\alpha X^\alpha$ 整除的多项式．证明 $f(X) - g(X)$ 的每个项都不被 $c_\alpha X^\alpha$ 整除．

6.83 由单项式生成的 $k[X]$ 中的理想 I，比如 $I = (X^{\alpha(1)}, \cdots, X^{\alpha(q)})$，叫做**单项式理想**．

（i）证明 $f(X) \in I$ 当且仅当 $f(X)$ 的每个项被某个 $X^{\alpha(i)}$ 整除．

（ii）证明：如果 $G = [g_1, \cdots, g_m]$ 和 r 是 $\bmod G$ 约化的，则 r 不在单项式理想 $(\mathrm{LT}(g_1), \cdots, \mathrm{LT}(g_m))$ 中．

6.84 设 $f(X) = \sum_\alpha c_\alpha X^\alpha \in k[X]$ 是对称多项式，其中 k 是域且 $X = (x_1, \cdots, x_n)$．假定 $\mathbb{N}^n$ 配置了次数-字典序且 $\mathrm{Deg}(f) = \beta = (\beta_1, \cdots, \beta_n)$．

（i）证明：如果 $c_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ 出现在 $f(X)$ 中，其中系数 c_α 非零，则每个单项式 $x_{\sigma_1}^{\alpha_1} \cdots x_{\sigma_n}^{\alpha_n}$ 都出现在 $f(X)$ 中且有非零系数，其中 $\sigma \in S_n$．

410

（ii）证明 $\beta_1 \geqslant \beta_2 \geqslant \cdots \geqslant \beta_n$．

（iii）如果 $e_1, \cdots, e_n$ 是初等对称多项式，证明

$$\mathrm{Deg}(e_i) = (1, \cdots, 1, 0, \cdots, 0),$$

其中有 i 个 1.

（iv）设 $(\gamma_1, \cdots, \gamma_n) = (\beta_1 - \beta_2, \beta_2 - \beta_3, \cdots, \beta_{n-1} - \beta_n, \beta_n)$．证明：如果 $g(x_1, \cdots, x_n) = x_1^{\gamma_1} \cdots x_n^{\gamma_n}$，则 $g(e_1, \cdots, e_n)$ 是对称多项式且 $\mathrm{Deg}(g) = \beta$.

（v）**对称多项式基本定理**．证明：如果 k 是域，则每个对称多项式 $f(X) \in k[X]$ 都是初等对称函数 $e_1, \cdots, e_n$ 的多项式．（与定理 4.37 比较．）

提示：证明 $h(X) = f(X) - c_\beta g(e_1, \cdots, e_n)$ 是对称的，且 $\mathrm{Deg}(h) < \beta$.

6.6.2 Buchberger 算法

本节的剩下部分我们假定 $\mathbb{N}^n$ 配置了某种单项序（读者可以用次数-字典序），由此 $\mathrm{LT}(f)$ 有定义且带余除法有意义．

我们已经看到由带余除法得到的 $f \bmod [g_1, \cdots, g_m]$ 的余式依赖于 g_i 列出的顺序．非正式地说，理想 $I = (g_1, \cdots, g_m)$ 的**格罗布纳基** $\{g_1, \cdots, g_m\}$ 是指一个生成集满足对 g_i 形成的每个 m 元组 $G_\sigma = [g_{\sigma(1)}, \cdots, g_{\sigma(m)}]$，$f \bmod G_\sigma$ 的余式恒为 f 进入 I 的阻碍，其中 $\sigma \in S_n$．我们用一个更易检验的性质来定义格罗布纳基，然后在命题 6.129 中证明它们被刚提到的更重要的阻碍性所刻画．

定义 多项式 $\{g_1,\cdots,g_m\}$ 的集合称为理想 $I=(g_1,\cdots,g_m)$ 的**格罗布纳基**[⊖]，如果对每个非零多项式 $f\in I$，存在某个 g_i 使得 $\mathrm{LT}(g_i)\mid \mathrm{LT}(f)$.

注意格罗布纳基是多项式集合，而不是多项式的 m 元组．例 6.128 证明了

$$\{y^2+z^2,x^2y+yz,z^3+xy\}$$

不是理想 (y^2+z^2,x^2y+yz,z^3+xy) 的格罗布纳基．

命题 6.129 一个多项式的集合 $(g_1,\cdots,g_m)$ 是理想 $I=(g_1,\cdots,g_m)$ 的格罗布纳基当且仅当对每个 m 元组 $G_\sigma=[g_{\sigma(1)},\cdots,g_{\sigma(m)}]$，其中 $\sigma\in S_m$，每个 $f\in I \bmod G_\sigma$ 的余式都为 0.

证明 假定有某个置换 $\sigma\in S_m$ 和某个 $f(X)=\sum_\alpha c_\alpha X^\alpha\in I$，$f \bmod G_\sigma$ 的余式不是 0. 将它的各项按多重次数降序排列，$\alpha_1\succ\cdots\succ\alpha_p$，并且如引理 6.123 的证明中一样，定义 $\mathrm{multiword}(f)=\alpha_1\cdots\alpha_p\in\mathcal{W}^+(\mathbf{N}^n)$．在所有这样的多项式 f 中，在良序集 $\mathcal{W}^+(\mathbf{N}^n)$ 中选择一个极小的．由于 $\{g_1,\cdots,g_m\}$ 是一个格罗布纳基，对某个 i 有 $\mathrm{LT}(g_i)\mid\mathrm{LT}(f)$．应用带余除法得到一个新多项式，比如说 h，注意 $h\in I$. 由于 $\mathrm{multidegree}(h)\prec\mathrm{multidegree}(f)$，根据命题 6.126，$h \bmod G_\sigma$ 的余式是 0. 因此，f 的余式也是 0，这是一个矛盾.

[411]

反之，假定每个 $f\in I$ 都有 $\bmod G_\sigma$ 的余式为 0，但 $\{g_1,\cdots,g_m\}$ 不是 $I=(g_1,\cdots,g_m)$ 的格罗布纳基．如果存在非零多项式 $f\in I$ 使得对每个 i 都有 $\mathrm{LT}(g_i)\nmid\mathrm{LT}(f)$，则在任一约化 $f\xrightarrow{g_i}h$ 中，有 $\mathrm{LT}(h)=\mathrm{LT}(f)$．因此，如果 $G=[g_1,\cdots,g_m]$，带余除法 $\bmod G$ 给出约化 $f\to h_1\to h_2\to\cdots\to h_p=r$，其中 $\mathrm{LT}(r)=\mathrm{LT}(f)$．所以 $r\neq 0$，即 $f \bmod G$ 的余式不是零，这是一个矛盾． ■

系 6.130 如果 $\{g_1,\cdots,g_m\}$ 是理想 $I=(g_1,\cdots,g_m)$ 的格罗布纳基，且 $G=[g_1,\cdots,g_m]$ 是 g_i 形成的任意一个 m 元组，则对每个 $f(X)\in k[X]$，存在唯一的 $\bmod\{g_1,\cdots,g_m\}$ 约化的 $r(X)\in k[X]$，使得 $f-r\in I$；事实上，r 是 $f \bmod G$ 的余式．

证明 带余除法给出 $\bmod\{g_1,\cdots,g_m\}$ 约化的多项式 r 和多项式 $a_1,\cdots,a_m$ 使得 $f=a_1g_1+\cdots+a_mg_m+r$，显然 $f-r=a_1g_1+\cdots+a_mg_m\in I$.

为证明唯一性，假设 r 和 r' 是 $\bmod\{g_1,\cdots,g_m\}$ 约化的且 $f-r$ 和 $f-r'$ 在 I 中，由此 $(f-r')-(f-r)=r-r'\in I$．因 r 和 r' 是 $\bmod\{g_1,\cdots,g_m\}$ 约化的，它们没有一个项能被 $\mathrm{LT}(g_i)$ 整除．如果 $r-r'\neq 0$，习题 6.82 说 $r-r'$ 的每个项都不能被任一 $\mathrm{LT}(g_i)$ 整除，特别是 $\mathrm{LT}(r-r')$ 不能被任一 $\mathrm{LT}(g_i)$ 整除，此与命题 6.129 矛盾，所以 $r=r'$. ■

下一个系证明格罗布纳基解决了由不同的 m 元组引起的带余除法中余式不同的问题．

系 6.131 设 $\{g_1,\cdots,g_m\}$ 是理想 $I=(g_1,\cdots,g_m)$ 的格罗布纳基，并设 $G=[g_1,\cdots,g_m]$.

（i）如果 $f(X)\in k[X]$ 和 $G_\sigma=[g_{\sigma(1)},\cdots,g_{\sigma(m)}]$，其中 $\sigma\in S_m$ 是置换，则 $f \bmod G$ 的余式等于 $f \bmod G_\sigma$ 的余式．

（ii）多项式 $f\in I$ 当且仅当 $f \bmod G$ 的余式为 0.

证明 （i）如果 r 是 $f \bmod G$ 的余式，则系 6.130 说 r 是 $\bmod\{g_1,\cdots,g_m\}$ 约化且满足 $f-r\in I$ 的唯一多项式．同样，$f \bmod G_\sigma$ 的余式 r_σ 是 $\bmod\{g_1,\cdots,g_m\}$ 约化且满足 $f-r_\sigma\in I$ 的唯一多项式．系 6.130 中的唯一性结论给出 $r=r_\sigma$.

⊖ 在 Buchberger-Winkler 的《Gröbner Bases and Applications》一书中，B. Buchberger 的一篇文章写道："在格罗布纳 1954 年的早期论文中，虽然没有包含格罗布纳基理论的基本成分，但给我指出了正确的方向，促使我在 1976 年给这个理论冠以格罗布纳的名字．"

（ⅱ）命题 6.129 证明：如果 $f \in I$，则它的余式是 0. 关于逆命题，如果 r 是 $f \bmod G$ 的余式，则 $f = q + r$，其中 $q \in I$. 因此如果 $r = 0$，则 $f \in I$. ■

有几个明显的问题．格罗布纳基是否存在，如果存在，是否唯一？给定 $k[X]$ 中的理想 I，有 [412] 没有求 I 的格罗布纳基的算法？

S-多项式的概念可以使我们识别格罗布纳基，先引入几个记号．

定义 如果 $\alpha = (\alpha_1, \cdots, \alpha_n)$ 和 $\beta = (\beta_1, \cdots, \beta_n)$ 在 $\mathbb{N}^n$ 中，定义

$$\alpha \vee \beta = \mu,$$

其中 $\mu_i = \max\{\alpha_i, \beta_i\}$ 和 $\mu = (\mu_1, \cdots, \mu_n)$．

注意 $X^{\alpha \vee \beta}$ 是单项式 X^α 和 X^β 的最小公倍式

定义 设 $f(X), g(X) \in k[X]$，其中 $\mathrm{LT}(f) = a_\alpha X^\alpha$ 和 $\mathrm{LT}(g) = b_\beta X^\beta$．定义

$$L(f,g) = X^{\alpha \vee \beta}.$$

S-多项式 $S(f,g)$ 定义为

$$S(f,g) = \frac{L(f,g)}{\mathrm{LT}(f)} f - \frac{L(f,g)}{\mathrm{LT}(g)} g;$$

即如果 $\mu = \alpha \vee \beta$，则

$$S(f,g) = a_\alpha^{-1} X^{\mu-\alpha} f(X) - b_\beta^{-1} X^{\mu-\beta} g(X).$$

注意 $S(f,g) = -S(g,f)$．

例 6.132 （ⅰ）如果 $f(x,y) = 3x^2y$ 和 $g(x,y) = 5xy^3 - y$（在次数-字典序中），则 $L(f,g) = x^2y^3$ 和

$$S(f,g) = \frac{x^2y^3}{3x^2y} 3x^2y - \frac{x^2y^3}{5xy^3}(5xy^3 - y) = \frac{1}{5}xy.$$

（ⅱ）如果 $f(X)$ 和 $g(X)$ 都是单项式，比如 $f(X) = a_\alpha X^\alpha$ 和 $g(X) = b_\beta X^\beta$，则

$$S(f,g) = \frac{X^{\alpha \vee \beta}}{a_\alpha X^\alpha} a_\alpha X^\alpha - \frac{X^{\alpha \vee \beta}}{b_\beta X^\beta} b_\beta X^\beta = 0.$$ ■

下面的技术性引理指出定义 S-多项式为什么是合适的．它说如果 $\mathrm{Deg}\left(\sum_j a_j g_j\right) < \delta$，其中 a_j 是单项式，而对一切 j，$\mathrm{Deg}(a_j g_j) = \delta$，则任一多元次数 $< \delta$ 的多项式可以重写为 S-多项式的线 [413] 性组合，它具有单项式系数，且它的每一项的多元次数严格小于 δ.

引理 6.133 给定 $g_1(X), \cdots, g_\ell(X) \in k[X]$ 和单项式 $c_j X^{\alpha(j)}$，令 $h(X) = \sum_{j=1}^{\ell} c_j X^{\alpha(j)} g_j(X)$．设 δ 是多元次数．如果 $\mathrm{Deg}(h) < \delta$ 和对一切，$j \leqslant \ell$，$\mathrm{Deg}(c_j X^{\alpha(j)} g_j(X)) = \delta$，则存在 $d_j \in k$ 使得

$$h(X) = \sum_j d_j X^{\delta - \mu(j)} S(g_j, g_{j+1}),$$

其中 $\mu(j) = \mathrm{Deg}(g_j) \vee \mathrm{Deg}(g_{j+1})$，且对一切 $j < \ell$，

$$\mathrm{Deg}(X^{\delta-\mu(j)} S(g_j, g_{j+1})) < \delta.$$

证明 设 $\mathrm{LT}(g_j) = b_j X^{\beta(j)}$，于是 $\mathrm{LT}(c_j X^{\alpha(j)} g_j(X)) = c_j b_j X^\delta$．从而 $h(X)$ 中 X^δ 的系数是 $\sum_j c_j b_j$．因 $\mathrm{Deg}(h) < \delta$，必有 $\sum_j c_j b_j = 0$．定义首一多项式

$$u_j(X) = b_j^{-1} X^{\alpha(j)} g_j(X).$$

有一个重叠和

$$
\begin{aligned}
h(X) &= \sum_{j=1}^{\ell} c_j X^{\alpha(j)} g_j(X) \\
&= \sum_{j=1}^{\ell} c_j b_j u_j \\
&= c_1 b_1 (u_1 - u_2) + (c_1 b_1 + c_2 b_2)(u_2 - u_3) + \cdots \\
&\quad + (c_1 b_1 + \cdots + c_{\ell-1} b_{\ell-1})(u_{\ell-1} - u_\ell) \\
&\quad + (c_1 b_1 + \cdots + c_\ell b_\ell) u_\ell .
\end{aligned}
$$

因 $\sum_j c_j b_j = 0$，所以最后一项 $(c_1 b_1 + \cdots + c_\ell b_\ell) u_\ell = 0$．因 $\delta = \mathrm{Deg}\,(c_j X^{\alpha(j)} g_j(X))$，所以有 $\alpha(j) + \beta(j) = \delta$，从而对一切 j，$X^{\beta(j)} \mid X^\delta$．因此对一切 $j < \ell$，有 $\mathrm{lcm}\,\{X^{\beta(j)}, X^{\beta(j+1)}\} = X^{\beta(j) \vee \beta(j+1)} \mid X^\delta$；即如果记 $\mu(j) = \beta(j) \vee \beta(j+1)$，则 $\delta - \mu(j) \in \mathbf{N}^n$．但

$$
\begin{aligned}
X^{\delta-\mu(j)} S(g_j, g_{j+1}) &= X^{\delta-\mu(j)} \left(\frac{X^{\mu(j)}}{\mathrm{LT}(g_j)} g_j(X) - \frac{X^{\mu(j)}}{\mathrm{LT}(g_{j+1})} g_{j+1}(X) \right) \\
&= \frac{X^\delta}{\mathrm{LT}(g_j)} g_j(X) - \frac{X^\delta}{\mathrm{LT}(g_{j+1})} g_{j+1}(X) \\
&= b_j^{-1} X^{\alpha(j)} g_j - b_{j+1}^{-1} X^{\alpha(j+1)} g_{j+1} \\
&= u_j - u_{j+1}.
\end{aligned}
$$

把这个等式代入重叠和中得所求的那种形式的和，其中 $d_j = c_1 b_1 + \cdots + c_j b_j$：

$$
\begin{aligned}
h(X) &= c_1 b_1 X^{\delta-\mu(1)} S(g_1, g_2) + (c_1 b_1 + c_2 b_2) X^{\delta-\mu(2)} S(g_2, g_3) + \cdots \\
&\quad + (c_1 b_1 + \cdots + c_{\ell-1} b_{\ell-1}) X^{\delta-\mu(\ell-1)} S(g_{\ell-1}, g_\ell).
\end{aligned}
$$

414

最后，因 u_j 和 u_{j+1} 都是首一的且首项多元次数为 δ，有 $\mathrm{Deg}(u_j - u_{j+1}) \prec \delta$．而我们已经证明 $u_j - u_{j+1} = X^{\delta-\mu(j)} S(g_j, g_{j+1})$，因此 $\mathrm{Deg}(X^{\delta-\mu(j)} S(g_j, g_{j+1})) \prec \delta$． ■

由命题 6.129，$\{g_1, \cdots, g_m\}$ 是 $I = (g_1, \cdots, g_m)$ 的格罗布纳基，如果对每个 $f \in I$，$f \bmod G$ 的余式为 0（其中 G 是排列 g_i 形成的任意 m 元组）．下一定理的重要性在于它证明了只要计算有限个多项式的余式，就是 S - 多项式，就可判定 $\{g_1, \cdots, g_m\}$ 是否为格罗布纳基．

定理 6.134（Buchberger） *集合 $\{g_1, \cdots, g_m\}$ 是理想 $I = (g_1, \cdots, g_m)$ 的格罗布纳基当且仅当对一切 p, q，$S(g_p, g_q) \bmod G$ 的余式为 0，其中 $G = [g_1, \cdots, g_m]$．*

证明 显然 $S(g_p, g_q)$ 在 I 中，它是 g_p 和 g_q 的线性组合．如果 $G = \{g_1, \cdots, g_m\}$ 是格罗布纳基，则由命题 6.129，$S(g_p, g_q) \bmod G$ 的余式为 0.

反之，假定对一切 p, q，$S(g_p, g_q) \bmod G$ 的余式都是 0，我们需要证明对每个 $f \in I$，$f \bmod G$ 的余式为 0. 根据命题 6.129，只要证明：如果 $f \in I$，则有某个 i 使得 $\mathrm{LT}(g_i) \mid \mathrm{LT}(f)$．因 $f \in I = (g_1, \cdots g_m)$，我们可以记 $f = \sum_i h_i g_i$，从而

$$
\mathrm{Deg}(f) \preceq \max_i \{\mathrm{Deg}(h_i g_i)\}.
$$

如果等式成立，则有某个 i 使得 $\mathrm{Deg}(f) = \mathrm{Deg}(h_i g_i)$，从而命题 6.125 给出所要的 $\mathrm{LT}(g_i) \mid \mathrm{LT}(f)$. 所以可以假定有严格的不等式：$\mathrm{Deg}(f) \prec \max_i \{\mathrm{Deg}(h_i g_i)\}$．

多项式 f 可以有多种方式写成 g_i 的线性组合．当然一切表达式都形如 $f = \sum_i h_i g_i$，选取 $\delta = \max_i \{\mathrm{Deg}(h_i g_i)\}$ 极小的一个（因 $\preceq$ 是良序，所以是可能的）．如果 $\mathrm{Deg}(f) = \delta$，正如我们已知的，证明已经完成，所以可假定有严格不等式 $\mathrm{Deg}(f) \prec \delta$．记

$$f=\sum_{\substack{j\\ \mathrm{Deg}(h_jg_j)=\delta}} h_jg_j+\sum_{\substack{\ell\\ \mathrm{Deg}(h_\ell g_\ell)<\delta}} h_\ell g_\ell. \tag{7}$$

如果 $\mathrm{Deg}\left(\sum_j h_jg_j\right)=\delta$，则 $\mathrm{Deg}(f)=\delta$，产生矛盾；因此 $\mathrm{Deg}\left(\sum_j h_jg_j\right)\prec\delta$. 但在这个和中 X^δ 的系数是从它的首项得到的，从而

$$\mathrm{Deg}\left(\sum_j \mathrm{LT}(h_j)g_j\right)\prec\delta.$$

现在 $\sum_j \mathrm{LT}(h_j)g_j$ 是满足引理 6.133 假设的多项式，因而存在常数 d_j 和多元次数 $\mu(j)$ 使得

415

$$\sum_j \mathrm{LT}(h_j)g_j=\sum_j d_jX^{\delta-\mu(j)}S(g_j,g_{j+1}), \tag{8}$$

其中 $\mathrm{Deg}(X^{\delta-\mu(j)}S(g_j,g_{j+1}))\prec\delta$. ⊖

因每个 $S(g_j,g_{j+1})\bmod G$ 的余式为 0，带余除法给出 $a_{ji}(X)\in k[X]$ 使得 $S(g_j,g_{j+1})=\sum_i a_{ji}g_i$，其中对一切 j，i，$\mathrm{Deg}(a_{ji}g_i)\preceq\mathrm{Deg}(S(g_j,g_{j+1}))$，由此

$$X^{\delta-\mu(j)}S(g_j,g_{j+1})=\sum_i X^{\delta-\mu(j)}a_{ji}g_i.$$

所以，引理 6.133 给出

$$\mathrm{Deg}(X^{\delta-\mu(j)}a_{ji}g_i)\preceq\mathrm{Deg}(X^{\delta-\mu(j)}S(g_j,g_{j+1}))\prec\delta. \tag{9}$$

代入（8）式得

$$\begin{aligned}\sum_j \mathrm{LT}(h_j)g_j&=\sum_j d_jX^{\delta-\mu(j)}S(g_j,g_{j+1})\\&=\sum_j d_j\left(\sum_i X^{\delta-\mu(j)}a_{ji}g_i\right)\\&=\sum_i\left(\sum_j d_jX^{\delta-\mu(j)}a_{ji}\right)g_i.\end{aligned}$$

如果记 $\sum_j d_jX^{\delta-\mu(j)}a_{ji}$ 为 h'_i，则

$$\sum_j \mathrm{LT}(h_j)g_j=\sum_i h'_ig_i, \tag{10}$$

其中，根据（9）式，对一切 i，$\mathrm{Deg}(h'_ig_i)\prec\delta$.

最后，把（10）式的表达式代入等式（7）：

$$\begin{aligned}f&=\sum_{\substack{j\\ \mathrm{Deg}(h_jg_j)=\delta}} h_jg_j+\sum_{\substack{\ell\\ \mathrm{Deg}(h_\ell g_\ell)<\delta}} h_\ell g_\ell\\&=\sum_{\substack{j\\ \mathrm{Deg}(h_jg_j)=\delta}} \mathrm{LT}(h_j)g_j+\sum_{\substack{j\\ \mathrm{Deg}(h_jg_j)=\delta}}[h_j-\mathrm{LT}(h_j)]g_j+\sum_{\substack{\ell\\ \mathrm{Deg}(h_\ell g_\ell)<\delta}} h_\ell g_\ell\\&=\sum_i h'_ig_i+\sum_{\substack{j\\ \mathrm{Deg}(h_jg_j)=\delta}}[h_j-\mathrm{LT}(h_j)]g_j+\sum_{\substack{\ell\\ \mathrm{Deg}(h_\ell g_\ell)<\delta}} h_\ell g_\ell.\end{aligned}$$

我们已经把 f 重写为 g_i 的线性组合，其中每个项的多元次数都严格小于 δ，与 δ 的极小性矛盾．证明完成． ■

416

系 6.135 如果 $I=(f_1,\cdots,f_s)$ 在 $k[X]$ 中，其中每个 f_i 都是单项式（即如果 I 是单项式理想），则 $\{f_1,\cdots,f_s\}$ 是 I 的格罗布纳基．

⊖ 读者会奇怪为什么我们考虑所有的 S-多项式 $S(g_p,g_q)$，而不是只考虑形如 $S(g_i,g_{i+1})$ 的 S-多项式．答案是余式条件只适用于满足 $\mathrm{Deg}(h_jg_j)=\delta$ 的那些 h_jg_j，从而记作 i 的指标未必是连续的．

证明 根据例6.132(ii)，任一单项式对的 S-多项式都是 0. ■

这里是主要结果：$(f_1,\cdots,f_s)$ 的格罗布纳基可以通过添加 S-多项式的余式获得.

定理 6.136 (Buchberger 算法) *$k[X]$ 中的每个理想 $I=(f_1,\cdots,f_s)$ 都有格罗布纳基*[⊖]，*它可以用一个算法计算出来.*

证明 下面是算法的伪码.

```
Input: B = {f_1,…,f_s}   G = [f_1,…,f_s]
Output: a Gröbner basis B = {g_1,…,g_m} containing {f_1,…,f_s}
B := {f_1,…,f_s}   G := [f_1,…,f_s]
REPEAT
    B' := B   G' := G
    FOR each pair g, g' with g ≠ g' ∈ B' DO
        r := remainder of S(g,g') mod G'
        IF r ≠ 0
          THEN B := B ∪ {r} and G' = [g_1,…,g_m,r]
UNTIL B = B'
```

现在算法的每个循环扩大子集 $B\subseteq I=(g_1,\cdots,g_m)$，它加进了 S-多项式 $S(g,g')$ 之一 mod G 的余式. 因 $g,g'\in I$，$S(g,g')$ 的余式在 I 中，从而大集 $B\cup\{r\}$ 包含在 I 中.

唯一阻碍算法在 B' 处终止的条件是有某个 $S(g,g')$ mod G' 的余式不为 0. 由此，如果算法终止，则定理 6.134 表明 B' 是格罗布纳基.

为证明该算法有终止，假设从 B' 开始以 B 结束. 因 $B'\subseteq B$，所以有单项式理想的包含关系

$$(\mathrm{LT}(g'):g'\in B')\subseteq(\mathrm{LT}(g):g\in B).$$

我们断言：如果 $B'\subsetneq B$，则也存在理想的严格包含关系. 假设 r 是某个 S-多项式 mod B' 的（非零）余式，且 $B=B'\cup\{r\}$. 根据定义，余式 r 是 mod G' 约化的，从而对任一 $g'\in B'$，r 的每个项都不能被 $\mathrm{LT}(g')$ 整除，特别是 $\mathrm{LT}(r)$ 不能被任何 $\mathrm{LT}(g')$ 整除. 因此，根据习题 6.83，$\mathrm{LT}(r)\notin(\mathrm{LT}(g'):g'\in B')$. 另一方面，我们有 $\mathrm{LT}(r)\in(\mathrm{LT}(g):g\in B)$. 所以，如果算法不终止，则存在 $k[X]$ 中理想的无限严格升链，因为 $k[X]$ 有 ACC，所以与希尔伯特基定理矛盾. ■ [417]

例 6.137 读者可以证明 $B'=\{y^2+z^2,x^2y+yz,z^3+xy\}$ 不是格罗布纳基，因为 $S(y^2+z^2,x^2y+yz)=x^2z^2-y^2z$ mod G' 的余式不是 0. 然而加进 $x^2z^2-y^2z$ 给出了一个格罗布纳基 B，因为 B 中一切 S-多项式［它们有 $\binom{4}{2}=6$ 个］mod B' 的余式都是 0. ■

理论上，Buchberger 算法可以计算格罗布纳基，但问题是如何实现. 在很多情形中，计算所需的时间在合理的范围之内，而另一方面，存在耗时很长才能产生输出的例子. 在 Cax-Little-O'Shea 的《Ideals，Varieties，and Algorithms》中 2.9 节讨论了 Buchberger 算法的效率.

系 6.138 (i) *如果 $I=(f_1,\cdots,f_t)$ 是 $k[X]$ 中的理想，则存在算法判定多项式 $h(X)\in k[X]$ 是否在 I 中.*

(ii) *如果 $I=(f_1,\cdots,f_t)\subseteq k[X]$，则存在算法判定多项式 $g(X)\in k[X]$ 是否在 $\sqrt{I}$ 中.*

⊖ 格罗布纳基存在的一个非构造性证明可以用希尔伯特基定理的证明给出，例如可见 Cox-Little-O'Shea 的《Ideals，Varieties，and Algorithms》第 2.5 节（在 2.7 节中，他们也给出一个构造性证明）.

（ⅲ）如果 $I=(f_1,\cdots,f_t)$ 和 $I'=(f_1',\cdots,f_s')$ 是 $k[X]$ 中的理想，则存在算法判定是否有 $I=I'$.

证明 （ⅰ）用 Buchberger 算法求出 I 的格罗布纳基 B，然后用带余除法计算 $h \bmod G$ 的余式（其中 G 是排列 B 中的多项式形成的任一 m 元组）．根据系 6.131(ⅱ)，$h\in I$ 当且仅当 $r=0$.

（ⅱ）用习题 6.66，然后用 Buchberger 算法求出 $k[X,y]$ 中 $(f_1,\cdots,f_t,1-yg)$ 的格罗布纳基．

（ⅲ）用 Buchberger 算法分别求出 I 和 I' 的格罗布纳基 $\{g_1,\cdots,g_m\}$ 和 $\{g_1',\cdots,g_m'\}$．根据（ⅰ），存在算法判定是否有每个 $g_j'\in I$，如果每个 $g_j'\in I$，则 $I'\subseteq I$．同样，存在算法判定相反的包含关系，因此存在算法判定是否有 $I=I'$． ■

一个格罗布纳基 $B=\{g_1,\cdots,g_m\}$ 可能太大．例如由格罗布纳基的定义，如果 $f\in I$，则 $B\cup\{f\}$ 也是 I 的格罗布纳基，由此，我们可以寻找在某种意义下极小的格罗布纳基．

定义 称理想 I 的基 $\{g_1,\cdots,g_m\}$ 是**约化的**，如果

（ⅰ）每个 g_i 都是首一的；

（ⅱ）每个 g_i 都是 $\bmod\{g_1,\cdots,\hat{g}_i,\cdots,g_m\}$ 约化的．

418

习题 6.90 给出一个算法计算每个理想 $(f_1,\cdots,f_t)$ 的约化基．结合习题 6.93 中的算法，它把一个格罗布纳基压缩为一个**约化格罗布纳基**，可以证明一个理想的约化格罗布纳基是唯一的．在每个 $f_i(X)$ 都是线性的特殊情形中，即

$$f_i(X)=a_{i1}x_1+\cdots+a_{in}x_n.$$

公共零点 $\mathrm{Var}(f_1,\cdots,f_t)$ 是 t 个方程 n 个未知数的齐次方程组的解．如果 $A=[a_{ij}]$ 是 $t\times n$ 系数矩阵，则可以证明约化格罗布纳基对应于矩阵 A 的行-约化梯矩阵（见 Becker-Weispfenning 所著的《Gröbner Bases》10.5 节）．另一种特殊情形是 $f_1,\cdots,f_t$ 都是一元多项式．从 $\{f_1,\cdots,f_t\}$ 得到的约化格罗布纳基是它们的 gcd，因此欧几里得算法已经推广到了多元多项式．

系 6.138 一开始没有说“如果 I 是 $k[X]$ 中的理想”，而是指定了一个基 $I=(f_1,\cdots,f_t)$．当然，其理由是 Buchberger 算法需要一个基作为输入．例如，如果 $J=(h_1,\cdots,h_s)$，则该算法不能直接用来检验多项式 $f(X)$ 是否在根 $\sqrt{J}$ 中，因为我们还没有 $\sqrt{J}$ 的基．Becker-Weispfenning 的书《Gröbner Bases》给出 k 满足某种条件时计算 $\sqrt{J}$ 的基的算法．没有已知的算法可以计算一个理想的相伴素理想，虽然有算法处理这个一般问题的几个特殊情形．正如我们在本节开始提到的，如果一个理想 I 有准素分解 $I=Q_1\cap\cdots\cap Q_r$，则相伴素理想 P_i 形如 $\sqrt{(I:c_i)}$，其中 $c_i\in\bigcap_{j\neq i}Q_j$ 且 $c_i\notin Q_i$．有算法计算冒号理想的基（Becker-Weispfenning 所著的《Gröbner Bases》，266 页）．于是，如果有求元素 c_i 的算法，就可以计算 P_i．对于格罗布纳基在数学各领域的应用的一个综述，读者可参见 Buchberger-Winkler 所著的《Gröbner Bases and Applications》．

我们通过呈示如何求理想之交的基来结束本章．

给定多元多项式方程组，求解该方程组的已知方法是消去变量（van der Waerden 所著的《Modern Algebra II》，第 XI 章）．给定一个理想 $I\in k[X]$，我们导出未定元的子集中的一个理想，它本质上是 $\mathrm{Var}(I)$ 和低维平面的交．

定义 设 k 是域，并设 $I\subseteq k[X,Y]$ 是理想，其中 $k[X,Y]$ 是变量的不相交集合 $X\cup Y$ 中的多项式环．**消元理想**是指

$$I_X=I\cap k[X].$$

例如，如果 $I=(x^2,xy)$，则一个格罗布纳基是 $\{x^2,xy\}$（它们是单项式，从而系 6.135 适

用)，而 $I_x=(x^2)\subseteq k[x], I_y=\{0\}$.

命题 6.139 设 k 是域，并设 $k[X]=k[x_1,\cdots,x_n]$ 有满足 $x_1>x_2>\cdots>x_n$ 的单项序（例如字典序），且对固定的 $p>1$，令 $Y=x_p,\cdots,x_n$. 如果 $I\subseteq k[X]$ 有格罗布纳基 $G=\{g_1,\cdots,g_m\}$，则 $G\cap I_Y$ 是消元理想 $I_Y=I\cap k[x_p,\cdots,x_n]$ 的格罗布纳基.

419

证明 回忆 $\{g_1,\cdots,g_m\}$ 是 $I=(g_1,\cdots,g_m)$ 的格罗布纳基意味着对每个非零 $f\in I$，存在 g_i 使得 $\mathrm{LT}(g_i)\mid\mathrm{LT}(f)$. 设 $f(x_p,\cdots,x_n)\in I_Y$ 是非零多项式. 因 $I_Y\subseteq I$，存在某个 $g_i(X)$ 使得 $\mathrm{LT}(g_i)\mid\mathrm{LT}(f)$，因此 $\mathrm{LT}(g_i)$ 只涉及"后面"的变量 $x_p,\cdots,x_n$. 令 $\mathrm{Deg}(\mathrm{LT}(g_i))=\beta$. 如果 g_i 有一个项 $c_\alpha X^\alpha$ 涉及"前面"的变量 x_i，其中 $i<p$，则因 $x_1>\cdots>x_p>\cdots>x_n$，因而有 $\alpha>\beta$. 因为 g_i 首项的次数 β 大于 g_i 其他项的次数，所以这是一个矛盾. 由此，$g_i\in k[x_p,\cdots,x_n]$. 现在习题 6.92 证明 $G\cap k[x_p,\cdots,x_n]$ 是 $I_Y=I\cap k[x_p,\cdots,x_n]$ 的格罗布纳基. ■

我们现在可以给出理想之交的格罗布纳基.

命题 6.140 设 k 是域，并设 $I_1,\cdots,I_t$ 是 $k[X]$ 中的理想，其中 $X=x_1,\cdots,x_n$.

（i）考虑有新变量 y_j(其中 $1\leqslant j\leqslant t$) 的多项式环 $k[X,y_1,\cdots,y_t]$. 如果 J 是由 $1-(y_1+\cdots+y_t)$ 和一切 y_jI_j 生成的 $k[X,y_1,\cdots,y_t]$ 中的理想，则 $\bigcap_{j=1}^{t} I_j=J_X$.

（ii）给定 $I_1,\cdots,I_t$ 的格罗布纳基，可以算出 $\bigcap_{j=1}^{t} I_j$ 的格罗布纳基.

证明 （i）如果 $f=f(X)\in J_X=J\cap k[X]$，则 $f\in J$，因此有等式

$$f(X)=g(X,Y)(1-\sum y_j)+\sum_j h_j(X,y_1,\cdots,y_t)y_jq_j(X),$$

其中 $g,h_j\in k[X,Y]$ 和 $q_j\in I_j$. 令 $y_j=1$ 和其他的 y 等于 0 得 $f=h_j(X,0,\cdots,1,\cdots,0)q_j(X)$. 注意 $h_j(X,0,\cdots,1,\cdots,0)\in k[X]$，从而 $f\in I_j$. 因 j 是任意的，我们有 $f\in\bigcap I_j$，由此 $J_X\subseteq\bigcap I_j$.

关于反包含，如果 $f\in\bigcap I_j$，则等式

$$f=f(1-\sum y_j)+\sum_j y_jf$$

表明所要的 $f\in J_X$.

（ii）用满足 X 中的一切变量都在 Y 中的变量之前的一个单项序，该结果便由（i）和命题 6.139 推出. ■

例 6.141 考虑理想 $I=(x)\cap(x^2,xy,y^2)\subseteq k[x,y]$，其中 k 是域，在例6.117(ii)中考虑过这个例. 尽管不难用手算求 I 的基，我们还是用格罗布纳基来说明命题 6.140. 设 u 和 v 是新变量，定义

$$J=(1-u-v,ux,ux^2,uxy,vy^2)\subseteq k[x,y,u,v].$$

第一步是求 J 的格罗布纳基，我们用满足 $x<y<u<v$ 的字典单项序. 因两个单项式的 S-多项式为 0，因此 Buchberger 算法很快给出 J 的格罗布纳基 G[⊖]：

420

$$G=\{v+u-1,x^2,yx,ux,uy^2-y^2\}.$$

由命题 6.139，I 的格罗布纳基是 $G\cap k[x,y]$：G 的一切不涉及变量 u 和 v 的那些元素. 于是，

$$I=(x)\cap(x^2,xy,y^2)=(x^2,xy).$$ ■

顺便提及格罗布纳基可以适用于非交换环. A. I. Shirsov 开始研究非交换多元多项式环是否存在类似的结果，其目的是实现算法以解决李代数中的问题.

⊖ 事实上这是习题 6.93 给出的约化格罗布纳基.

习题

在下面的习题中用次数-字典单项序.

6.85 设 $I=(y-x^2,z-x^3)$.

(i) 令 $x\prec y\prec z$，设 $\preceq_{\text{lex}}$ 是 $\mathbb{N}^3$ 上相应的单项序. 证明 $[y-x^2,z-x^3]$ 不是 I 的格罗布纳基.

(ii) 令 $y\prec z\prec x$，设 $\preceq_{\text{lex}}$ 是 $\mathbb{N}^3$ 上相应的单项序. 证明 $[y-x^2,z-x^3]$ 是 I 的格罗布纳基.

6.86 求 $I=(x^2-1,xy^2-x)$ 的格罗布纳基.

6.87 求 $I=(x^2+y,x^4+2x^2y+y^2+3)$ 的格罗布纳基.

6.88 求 $I=(xz,xy-z,yz-x)$ 的格罗布纳基. x^3+x+1 在 I 中吗?

6.89 求 $I=(x^2-y,y^2-x,x^2y^2-xy)$ 的格罗布纳基. x^4+x+1 在 I 中吗?

6.90 证明下列伪码给出理想 $I=(f_1,\cdots,f_t)$ 的约化基 Q.

```
Input: P=[f_1,…,f_t]
Output: Q=[q_1,…,q_s]
Q:=P
WHILE there is q∈Q which is
      not reduced mod Q−{q} DO
  select q∈Q which is not reduced mod Q−{q}
  Q:=Q−{q}
  h:=the remainder of q mod Q
  IF h≠0 THEN
    Q:=Q∪{h}
  END IF
END WHILE
make all q∈Q monic
```

421

6.91 如果 G 是理想 I 的格罗布纳基，Q 是由习题 6.90 中的算法得到的 I 的基，证明 Q 也是 I 的格罗布纳基.

6.92 设 I 是 $k[X]$ 中的理想，其中 k 是域且 $k[X]$ 有单项序. 证明：如果一个多项式集合 $\{g_1,\cdots,g_m\}\subseteq I$ 有如下的性质，即对每个非零 $f\in I$ 有某个 g_i 使得 $\text{LT}(g_i)\mid\text{LT}(f)$，则 $I=(g_1,\cdots,g_m)$. 由此推出，在格罗布纳基的定义中，不必假定 I 由 $g_1,\cdots,g_m$ 生成.

6.93 证明下面的伪码把一个格罗布纳基 G 变成一个约化格罗布纳基 H.

```
Input: G={g_1,…,g_m}
Output: H
H:=∅;  F:=G
WHILE F≠∅ DO
  select f' from F
  F:=F−{f'}
  IF LT(f)∤LT(f') for all f∈F AND
       LT(h)∤LT(f') for all h∈H THEN
    H:=H∪{f'}
  END IF
END WHILE
apply the algorithm in Exercise 6.90 to H
```

422

第7章 模和范畴

我们现在介绍 R-模，其中 R 是交换环；正式地说，它们是向量空间在下列意义上的推广，即允许标量在 R 中，而不要求在域中．如果 R 是一个 PID，则我们将在第 9 章中看到，有限生成的 R-模的分类同时给出了一切有限生成阿贝尔群的分类，以及由典范型构成的有限维向量空间上一切线性变换的分类．在第 8 章中引入非交换环之后，我们还要定义这些环上的模，在本质上，它们将用来证明每个 $p^m q^n$ 阶有限群都是可解群，其中 p 和 q 是素数．

范畴和函子最先在代数拓扑中产生，代数拓扑用某种相关的代数系统（同调群、上同调环、同伦群）来研究拓扑空间和连续映射．已经证明范畴的概念在纯代数中也有其价值，确实，公正地说，近来代数几何的大幅进展不能没有范畴的框架．

7.1 模

一个 R-模就是"环 R 上的向量空间"，即在向量空间的定义中，允许标量在 R 中而不必是在域中．

定义 设 R 是交换环．R-**模**是指配置了**标量乘法** $R \times M \to M$ 的（加法）阿贝尔群 M，其中标量乘法记为

$$(r,m) \mapsto rm,$$

且使得下列公理对一切 $m, m' \in M$ 和一切 $r, r', 1 \in R$ 都成立：

（ⅰ）$r(m+m') = rm + rm'$；

（ⅱ）$(r+r')m = rm + r'm$；

（ⅲ）$(rr')m = r(r'm)$；

（ⅳ）$1m = m$.

注 这个定义对非交换环 R 也有意义，此时称 M 为**左** R-**模**．

例 7.1 （ⅰ）域 k 上的每个向量空间都是 k-模．

（ⅱ）根据命题 2.23 的指数定律，每个阿贝尔群都是 $\mathbb{Z}$-模．

（ⅲ）每个交换环 R 都可以看作它自身上的模，只要定义标量乘法 $R \times R \to R$ 为给定的 R 中元素的乘法．更一般地，R 中的每个理想 I 都是一个 R-模，这是因为对 $i \in I$ 和 $r \in R$ 有 $ri \in I$．

（ⅳ）如果 S 是交换环 R 的子环，则 R 是 S-模，其中标量乘法 $S \times R \to R$ 就是给定的乘法 $(s,r) \mapsto sr$. 例如，如果 k 是交换环，则 $k[X]$ 是 k-模．

（ⅴ）设 $T: V \to V$ 是线性变换，其中 V 是域 k 上的有限维向量空间．向量空间 V 可以成为 $k[x]$-模，如果如下定义标量乘法 $k[x] \times V \to V$：如果 $f(x) = \sum_{i=0}^{m} c_i x^i$ 在 $k[x]$ 中，则

$$f(x)v = \Big(\sum_{i=0}^{m} c_i x^i\Big)v = \sum_{i=0}^{m} c_i T^i(v),$$

其中 T^0 是恒等映射 1_V，如果 $i \geqslant 1$，则 T^i 是 T 和它自身复合 i 次．把 V 看作 $k[x]$-模时，我们把它记为 V^T.

这里是这种结构的一个特殊情形．设 A 是元素在 k 中的 $n\times n$ 矩阵，并设 $T: k^n\to k^n$ 是线性变换 $T(w)=Aw$，其中 w 是 $n\times 1$ 列向量，Aw 是矩阵乘法．现在定义标量乘法 $k[x]\times k^n\to k^n$ 如下：如果 $f(x)=\sum_{i=0}^{m}c_ix^i\in k[x]$，则

$$f(x)w=\Big(\sum_{i=0}^{m}c_ix^i\Big)w=\sum_{i=0}^{m}c_iA^iw,$$

其中 $A^0=I$ 是单位矩阵，如果 $i\geqslant 1$，A^i 是 A 的 i 次幂．现在我们证明 $(k^n)^T=(k^n)^A$．两个模由同样的元素组成（即一切 n 元组），标量乘法相同：在 $(k^n)^T$ 中有 $xw=T(w)$，在 $(k^n)^A$ 中有 $xw=Aw$，因 $T(w)=Aw$，所以两者相同．■

下面是相应的同态的概念．

定义 如果 R 是环且 M，N 是 R-模，则称函数 $f: M\to N$ 为 R-**同态**（或 R-**映射**），如果对一切 $m,m'\in M$ 和一切 $r\in R$，

（ⅰ）$f(m+m')=f(m)+f(m')$；

424

（ⅱ）$f(rm)=rf(m)$．

如果一个 R-同态是双射，则称它为 R-**同构**．R-模 M 和 N 称为**同构的**，记为 $M\cong N$，如果存在某个 R-同构 $f: M\to N$．

注意 R-同态的复合是 R-同态，如果 f 是 R-同构，则它的逆函数 f^{-1} 也是 R-同构．

例 7.2 （ⅰ）如果 R 是域，则 R-模是向量空间，R-映射是线性变换．这里的同构是非奇异线性变换．

（ⅱ）由例7.1(ⅱ)，$\mathbb{Z}$-模就是阿贝尔群，引理 2.52 表明每个（阿贝尔）群的同态是 $\mathbb{Z}$-映射．

（ⅲ）如果 M 是 R-模和 $r\in R$，则乘 r（或扩大 r 倍）是指由 $m\mapsto rm$ 给出的函数 $\mu_r: M\to M$.

因为 R 是交换的，所以函数 μ_r 是 R-映射：如果 $a\in R$ 和 $m\in M$，则 $\mu_r(am)=ram$，而 $a\mu_r(m)=arm$.

（ⅳ）设 $T: V\to V$ 是域 k 上向量空间 V 的一个线性变换，设 $v_1,\cdots,v_n$ 是 V 的基，并设 A 是 T 关于这个基的矩阵．我们现在证明两个 $k[x]$-模 V^T 和 $(k^n)^A$ 同构．

定义 $\varphi: V\to k^n$ 为 $\varphi(v_i)=e_i$，其中 $e_1,\cdots,e_n$ 是 k^n 的标准基，线性变换 φ 是向量空间的同构．为证明 φ 是 $k[x]$-映射，只要证明对一切 $f(x)\in k[x]$ 和一切 $v\in V$ 有 $\varphi(f(x)v)=f(x)\varphi(v)$. 现在

$$\begin{aligned}\varphi(xv_i)&=\varphi(T(v_i))\\&=\varphi(\sum a_{ji}v_j)\\&=\sum a_{ji}\varphi(v_j)\\&=\sum a_{ji}e_j,\end{aligned}$$

它是 A 的第 i 列．另一方面，

$$x\varphi(v_i)=A\varphi(v_i)=Ae_i,$$

它也是 A 的第 i 列．由此对一切 $v\in V$ 有 $\varphi(xv)=x\varphi(v)$，对 $\deg(f)$ 用归纳法容易证明对一切 $f(x)\in k[x]$ 和一切 $v\in V$，有 $\varphi(f(x)v)=f(x)\varphi(v)$. ■

下一命题推广了最后一例．

命题 7.3 设 V 是域 k 上的向量空间，并设 $T,S: V\to V$ 是线性变换，则例7.1(ⅴ)中的 $k[x]$-模

V^T 和 V^S 是 $k[x]$ - 同构的当且仅当存在向量空间的同构 $\varphi: V \to V$ 使得

$$S = \varphi T \varphi^{-1}.$$

425

证明 如果 $\varphi: V^T \to V^S$ 是 $k[x]$ - 同构，则 $\varphi: V \to V$ 是向量空间的同构使得对一切 $v \in V$ 和 $f(x) \in k[x]$ 有

$$\varphi(f(x)v) = f(x)\varphi(v).$$

特别地，如果 $f(x) = x$，则

$$\varphi(xv) = x\varphi(v).$$

但 V^T 中标量乘法的定义是 $xv = T(v)$，而 V^S 中标量乘法的定义是 $xv = S(v)$. 因此对一切 $v \in V$ 有

$$\varphi(T(v)) = S(\varphi(v)).$$

所以，

$$\varphi T = S\varphi.$$

因 φ 是同构，所以可得要证明的等式 $S = \varphi T \varphi^{-1}$.

反之，在 $\deg(f) \leqslant 1$ 的特殊情形中可以假定 $\varphi(f(x)v) = f(x)\varphi(v)$：

$$\varphi(xv) = \varphi T(v) = S\varphi(v) = x\varphi(v).$$

其次，容易用归纳法证明 $\varphi(x^n v) = x^n \varphi(v)$，再对 $\deg(f)$ 用归纳法可以证明 $\varphi(f(x)v) = f(x)\varphi(v)$. ■

值得把这个命题的一个特殊情形表达得更清晰．下一个系证明矩阵的相似性多么轻松地适合模的语言（在第 9 章中会看到这个事实有助于寻找典范型）．

系 7.4 设 k 是域，并设 A 和 B 是元素在 k 中的 $n \times n$ 矩阵，则例7.1(Ⅴ)中的 $k[x]$ - 模 $(k^n)^A$ 和 $(k^n)^B$ 是 $k[x]$ - 同构的当且仅当存在非奇异矩阵 P 使得

$$B = PAP^{-1}.$$

证明 定义 $T: k^n \to k^n$ 为 $T(y) = Ay$，其中 $y \in k^n$ 是一个列向量，由例7.1(Ⅴ)，$k[x]$ - 模 $(k^n)^T = (k^n)^A$. 类似地，定义 $S: k^n \to k^n$ 为 $S(y) = By$，并记相应的 $k[x]$ - 模为 $(k^n)^B$. 现在命题 7.3 给出同构 $\varphi: V^T \to V^S$ 满足

$$\varphi(Ay) = B\varphi(y).$$

根据命题 3.94，存在 $n \times n$ 矩阵 P 使得对一切 $y \in k^n$ 有 $\varphi(y) = Py$（因为 φ 是同构，所以它是非奇异的）．所以对一切 $y \in k^n$，

$$PAy = BPy,$$

从而

$$PA = BP;$$

因此，$B = PAP^{-1}$.

反之，非奇异矩阵 P 给出同构 $\varphi: k^n \to k^n$ 为对一切 $y \in k^n$，$\varphi(y) = Py$. 现在命题 7.3 表明 $\varphi: (k^n)^A \to (k^n)^B$ 是 $k[x]$ - 模同构． ■

426

同态可以相加．

定义 如果 M 和 N 是 R-模，则

$$\mathrm{Hom}_R(M,N) = \{M \to N \text{ 的一切 } R\text{-同态}\}.$$

如果 $f,g \in \mathrm{Hom}_R(M,N)$，则定义 $f+g: M \to N$ 为

$$f+g: m \mapsto f(m)+g(m).$$

命题 7.5 如果 M 和 N 是 R-模，其中 R 是交换环，则 $\mathrm{Hom}_R(M,N)$ 是 R-模，其中加法是刚定义的，标量乘法由

$$rf: m \mapsto f(rm)$$

给出．此外，有分配律：如果 $p: M' \to M$ 和 $q: N \to N'$，则对一切 $f,g \in \mathrm{Hom}_R(M,N)$ 有

$$(f+g)p = fp+gp \quad 和 \quad q(f+g) = qf+qg.$$

证明 容易验证 R-模定义中的公理，我们只给出

$$(rr')f = r(r'f)$$

的证明，因为它用到了 R 的交换性．

如果 $m \in M$，则 $(rr')f: m \mapsto f(rr'm)$. 另一方面，$r(r'f): m \mapsto (r'f)(rm) = f(r'rm)$. 因 R 是交换的，所以 $rr' = r'r$，从而 $(rr')f = r(r'f)$. ■

例 7.6 在线性代数中，域 k 上向量空间 V 的**线性泛函**是线性变换 $\varphi: V \to k$［毕竟，k 是它自身上的（一维）向量空间］．例如，如果

$$V = \{连续函数\ f: [0,1] \to \mathbb{R}\},$$

则积分 $f \mapsto \int_0^1 f(t)\mathrm{d}t$ 是 V 上的线性泛函．

如果 V 是域 k 上向量空间，则它的**对偶空间**是指 V 上一切线性泛函的集合：

$$V^* = \mathrm{Hom}_k(V,k).$$

根据命题 7.5，V^* 也是 k-模，即 V^* 是 k 上的向量空间． ■

我们现在证明对阿贝尔群和对向量空间所建立的那些结构也可以用到模上．子模 S 是指包含在一个较大的 R-模 M 中的 R-模，它使得如果 $s,s' \in S$ 和 $r \in R$，则 $s+s'$ 和 rs 在 S 中和在 M 中有同样的意义．

定义 如果 M 是 R-模，则 M 的**子模** N 是指 M 的加法子群 N，它在标量运算下封闭：只要 $n \in N$ 且 $r \in R$ 就有 $rn \in N$，记为 $N \subseteq M$.

427

例 7.7 （i）$\{0\}$ 和 M 都是模 M 的子模．M 的**真子模**是指子模 $N \subseteq M$ 且 $N \neq M$. 此时，我们可以写作 $N \subsetneq M$.

（ii）如果把交换环 R 看作它自身上的模，则 R 的子模是理想，当 I 是真理想时，它是真子模．

（iii）$\mathbb{Z}$-模（即阿贝尔群）的子模是子群，向量空间的子模是子空间．

（iv）如果 $T: V \to V$ 是线性变换，则 V^T 的子模 W 是 V 的子空间 W 满足 $T(W) \subseteq W$（子模显然具有这个性质，逆命题作为习题留给读者）．这样的子空间称为**不变子空间**．

（v）假设 R 是一个交换环．如果 M 是 R-模和 $r \in R$，则

$$rM = \{rm : m \in M\}$$

是 M 的子模．

这儿有一个相关结构．如果 J 是 R 中的理想，M 是 R-模，则

$$JM = \left\{\sum_i j_i m_i : j_i \in J \text{ 和 } m_i \in M\right\}$$

是 M 的子模．

（vi）如果 S 和 T 都是模 M 的子模，则

$$S+T=\{s+t : s\in S \text{和} t\in T\}$$

是包含 S 和 T 的 M 的子模.

(vii) 如果 $\{S_i : i\in I\}$ 是模 M 的子模族，则 $\bigcap_{i\in I} S_i$ 也是 M 的子模.

(viii) 如果 M 是 R-模和 $m\in M$，则由 **m 生成的循环子模**（记为 $\langle m\rangle$）是指

$$\langle m\rangle=\{rm : r\in R\}.$$

更一般地，如果 X 是 R-模 M 的子集，则

$$\langle X\rangle=\left\{\sum_{\text{有限}} r_ix_i : r_i\in R \text{和} x_i\in X\right\},$$

即 X 中元素的一切 **R-线性组合的集合**. 称 $\langle X\rangle$ 为**由 X 生成的子模**. 见习题 7.2. ■

定义 称模 M 是**有限生成的**，如果 M 由一个有限集生成，即存在有限子集 $X=\{x_1,\cdots,x_n\}$ 使得 $M=\langle X\rangle$.

例如，向量空间是有限生成的当且仅当它是有限维向量空间.

我们继续把有关阿贝尔群和有关向量空间的定义扩展到模. [428]

定义 如果 $F : M\to N$ 是 R-模之间的 R-映射，则

$$f \text{ 的核}=\ker f=\{m\in M : f(m)=0\}$$

和

$$f \text{ 的象}=\operatorname{im} f=\{n\in N : \text{存在 } m\in M \text{ 使得 } n=f(m)\}.$$

容易验证 $\ker f$ 是 M 的子模以及 $\operatorname{im} f$ 是 N 的子模. 假设 $M=\langle X\rangle$，即 M 由子集 X 生成. 进一步假设 N 是模且 $f,g : M\to N$ 是 R-同态. 如果 f 和 g 在 X 上一致 [即对一切 $x\in X$ 有 $f(x)=g(x)$]，则 $f=g$. 理由是由 $f-g : m\mapsto f(m)-g(m)$ 定义的 $f-g : M\to N$ 是 R-同态满足 $X\subseteq \ker(f-g)$. 所以 $M=\langle X\rangle\subseteq \ker(f-g)$，从而 $f-g$ 恒等于零；即 $f=g$.

定义 如果 N 是 R-模 M 的子模，则**商模**是指商群 M/N（回忆 M 是阿贝尔群，N 是子群）配置以标量乘法

$$r(m+N)=rm+N.$$

易知由 $m\mapsto m+N$ 给出的**自然映射** $\pi : M\to M/N$ 是 R-映射.

商模定义中的标量乘法是合理定义的：如果 $m+N=m'+N$，则 $m-m'\in N$，因此 $r(m-m')\in N$（因为 N 是子模），从而 $rm-rm'\in N$ 且 $rm+N=rm'+N$.

定理 7.8（第一同构定理） 如果 $f : M\to N$ 是模的 R-映射，则存在 R-同构

$$\varphi : M/\ker f\to \operatorname{im} f,$$

它由

$$\varphi : m+\ker f\mapsto f(m)$$

给出.

证明 如果我们把 M 和 N 仅仅看作阿贝尔群，则群的第一同构定理说 $\varphi : M/\ker f\to \operatorname{im} f$ 是阿贝尔群的同构. 但 φ 是 R-映射：$\varphi(r(m+N))=\varphi(rm+N)=f(rm)$. 然而因 f 是 R-映射，所以正如所要的 $f(rm)=rf(m)=r\varphi(m+N)$. ■

第二和第三同构定理是第一同构定理的推论.

定理 7.9（第二同构定理） 如果 S 和 T 是模 M 的子模，则存在 R-同构

$$S/(S\cap T)\to(S+T)/T.$$

证明 设 $\pi: M\to M/T$ 是自然映射，从而 $\ker\pi = T$；定义 $h=\pi|S$，从而 $h: S\to M/T$. 现在

429

$$\ker h = S\cap T$$

和

$$\operatorname{im} h = (S+T)/T$$

[因为 $(S+T)/T$ 由 M/T 中代表元在 S 中的那些陪集组成]. 现在应用第一同构定理可得结论. ■

定理 7.10（第三同构定理） 如果 $T\subseteq S\subseteq M$ 是子模的塔，则存在 R-同构

$$(M/T)/(S/T)\to M/S.$$

证明 定义映射 $g: M/T\to M/S$ 是**陪集扩大**；即

$$g: m+T\mapsto m+S.$$

现在 g 是合理定义的：如果 $m+T=m'+T$，则 $m-m'\in T\subseteq S$，从而 $m+S=m'+S$. 此外，

$$\ker g = S/T$$

和

$$\operatorname{img} = M/S.$$

运用第一同构定理完成证明. ■

如果 $f: M\to N$ 是模的映射且 $S\subseteq N$，则读者可以验证

$$f^{-1}(S)=\{m\in M: f(m)\in S\}$$

是包含 $\ker f$ 的 M 的子模.

定理 7.11（对应定理） 如果 T 是模 M 的子模，则存在双射

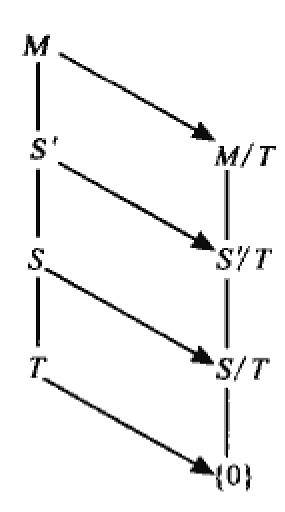
$$\varphi:\ \{\text{中间子模 } T\subseteq S\subseteq M\}\to\{M/T \text{ 的子模}\},$$

它由

$$S\mapsto S/T$$

430

给出. 此外，在 M 中 $S\subseteq S'$ 当且仅当在 M/T 中 $S/T\subseteq S'/T$.



证明 因每个模都是加法阿贝尔群，所以每个子模是子群，因此定理 2.76，即群的对应定理表明 φ 是保持包含关系的单射：在 M 中 $S\subseteq S'$ 当且仅当在 M/T 中 $S/T\subseteq S'/T$. 这个证明的剩余部分是命题 6.1 证明的简单修改；只要验证加性同态是现在的 R-映射. ■

命题 7.12 R-模 M 是循环模当且仅当有某个理想 I 使得 $M\cong R/I$.

证明 如果 M 是循环模，则有某个 $m\in M$ 使得 $M=\langle m\rangle$. 定义 $f: R\to M$ 为 $f(r)=rm$. 现

在因 M 是循环模，所以 f 是满射，它的核是某个理想 I. 第一同构定理给出 $R/I \cong M$.

反之，R/I 是循环的，生成元为 $1+I$，和循环模同构的任一模也是循环模． ■

定义 称模 M 为**单模**（或**不可约的**），如果 $M \neq \{0\}$ 且 M 没有非零真子模，即 M 的子模只有 $\{0\}$ 和 M.

例 7.13 根据命题 2.107，阿贝尔群 G 是单模当且仅当有某个素数 p 使得 $G \cong \mathbb{I}_p$. ■

系 7.14 R-模 M 是单模当且仅当 $M \cong R/I$，其中 I 是极大理想．

证明 由对应定理可得结果． ■ [431]

这样，极大理想的存在性保证了单模的存在性．

直和的概念已经在向量空间和阿贝尔群中讨论过，现在将其推广到模．回忆一个阿贝尔群 G 是子群 S 和 T 的内直和，如果 $S+T=G$ 且 $S \cap T=\{0\}$，而外直和是这样一个阿贝尔群，它的底集是笛卡儿积 $S \times T$，它的二元运算是点态加法，两种定义给出同构的阿贝尔群．内-外直和的观点在模中依然存在．

定义 如果 S 和 T 是 R-模，其中 R 是交换环[⊖]，则它们的**直和**是指笛卡儿积 $S \times T$ 配置以坐标形态的运算：

$$(s,t)+(s',t')=(s+s',t+t');$$
$$r(s,t)=(rs,rt),$$

其中 $s,s' \in S, t,t' \in T, r \in R$. S 和 T 的直和记为[⊜]$S \sqcup T$.

存在单射 R-映射 $\lambda_S: S \to S \sqcup T$ 和 $\lambda_T: T \to S \sqcup T$，它们分别由 $\lambda_S: S \mapsto (s,0)$ 和 $\lambda_T: t \mapsto (0,t)$ 给出．

命题 7.15 对 R-模 M，S 和 T，下列陈述等价．

(i) $S \sqcup T \cong M$.

(ii) 存在单射 R-映射 $i: S \to M$ 和 $j: T \to M$ 使得

$$M = \operatorname{im} i + \operatorname{im} j \text{ 和 } \operatorname{im} i \cap \operatorname{im} j = \{0\}.$$

(iii) 存在 R-映射 $i: S \to M$ 和 $j: T \to M$ 使得对每个 $m \in M$，存在唯一的 $s \in S$ 和 $t \in T$ 满足

$$m = is + jt.$$

(iv) 存在 R-映射 $i: S \to M, j: T \to M, p: M \to S$ 和 $q: M \to T$ 满足

$$pi = 1_S, \quad qj = 1_T, pj = 0, qi = 0, \text{和 } ip + jq = 1_M.$$

注 称映射 i 和 j 为**内射**，称映射 p 和 q 为**投射**．等式 $pi = 1_S$ 和 $qj = 1_T$ 表明映射 i 和 j 必是单射（因此 $\operatorname{im} i \cong S$ 和 $\operatorname{im} j \cong T$），映射 p 和 q 必是满射． [432]

证明 (i) ⇒ (ii) 设 $\varphi: S \sqcup T \to M$ 是同构，并定义 $i = \varphi\lambda_S$ [其中 $\lambda_S: s \mapsto (s,0)$] 和 $j = \varphi\lambda_T$ [其中 $\lambda_T: t \mapsto (0,t)$]. i 和 j 都是单射的复合，因此也都是单射．如果 $m \in M$，则有唯一的有序对 $(s, t) \in S \sqcup T$ 使得 $m = \varphi((s,t))$. 因此

$$m = \varphi((s,t)) = \varphi((s,0)+(0,t)) = \varphi\lambda_S(s) + \varphi\lambda_T(t) = is + jt \in \operatorname{im} i + \operatorname{im} j.$$

如果 $x \in \operatorname{im} i \cap \operatorname{im} j$，则有 $s \in S$ 和 $t \in T$ 使得 $is = jt$；即 $\varphi\lambda_S(s) = \varphi\lambda_T(t)$. 因 φ 是同构，在 $S \sqcup T$ 中有 $(s,0) = \lambda_S(s) = \lambda_T(t) = (0,t)$. 所以，$s = 0 = t$，$x = 0$ 和 $\operatorname{im} i \cap \operatorname{im} j = \{0\}$.

⊖ 下一章定义非交换环上的模．

⊜ 其他常用记号是 $S \oplus T$ 和 $S \times T$.

(ⅱ) ⇒ (ⅲ) 给定 $m\in M$，根据（ⅱ），存在形如 $m=is+jt$ 的表达式，因此我们只需证明唯一性．如果也有 $m=is'+jt'$，则 $i(s-s')=j(t'-t)\in \mathrm{im}i\cap \mathrm{im}j=\{0\}$．所以 $i(s-s')=0$ 和 $j(t-t')=0$. 因 i 和 j 都是单射，所以有 $s=s'$ 和 $t=t'$．

(ⅲ) ⇒ (ⅳ) 如果 $m\in M$，则存在唯一的 $s\in S$ 和 $t\in T$ 使得 $m=is+jt$．于是由

$$p(m)=s \text{ 和 } q(m)=t$$

定义的函数 p 和 q 是合理定义的．容易验证 p 和 q 是 R-映射，并且陈述中前四个等式成立(它们由 p 和 q 的定义而得). 关于最后一个等式，如果 $m\in M$，则 $m=is+jt$，$ip(m)+jq(m)=is+jt=m$.

(ⅳ) ⇒ (ⅰ) 定义 $\varphi: S\sqcup T\to M$ 为 $\varphi:(s,t)\mapsto is+jt$．易知 φ 是 R-映射，因 $1_M=ip+jq$，所以 φ 是满射．为证明 φ 是单射，假设 $\varphi((s,t))=0$，从而 $is=-jt$. 现在正如所要的，$s=pis=-pjt=0$ 和 $-t=-qjt=qis=0$． ■

内直和或许是一个模同构于一个直和的最重要的情形．

定义 设 S 和 T 都是模 M 的子模．如果 $M\cong S\sqcup T$，且 $i: S\to M$ 和 $j: T\to M$ 是包含映射，则称 M 是 S 和 T 的**内直和**．记内直和为

$$M=S\oplus T.$$

仅在本章中我们使用记号 $S\sqcup T$ 来表示外直和（底集是一切有序对的笛卡儿积），并使用记号 $M=S\oplus T$ 表示内直和（如刚才定义的，S 和 T 是 M 的子模）．稍后，我们将使用和数学界一样的写法：两种直和都用同一个记号 $S\oplus T$ 表示．

下面是命题 7.15 对内直和的重述．

系 7.16 对 R-模 M 及其子模 S 和 T，下列条件等价．

[433]

(ⅰ) $M=S\oplus T$.

(ⅱ) $S+T=M$ 和 $S\cap T=\{0\}$.

(ⅲ) 每个 $m\in M$ 都有唯一的形如 $m=s+t$ 的表达式，其中 $s\in S$ 和 $t\in T$.

证明 取 i 和 j 为包含映射，立刻可从命题 7.15 得证． ■

定义 称模 M 的一个子模 S 为 M 的**直和项**，如果存在 M 的子模 T 使得 $M=S\oplus T$.

下一个系把直和项与一种特殊的同态联系起来．

定义 如果 S 是 R-模 M 的子模，则称 S 是 M 的**收缩核**，如果存在叫做**收缩**的 R-同态 $\rho: M\to S$ 使得对一切 $s\in S$ 有 $\rho(s)=s$.

收缩在习题 5.72 的非阿贝尔群中出现过．

系 7.17 模 M 的子模 S 是直和项当且仅当存在收缩 $\rho: M\to S$.

证明 这里令 $i: S\to M$ 是包含映射．我们证明 $M=S\oplus T$，其中 $T=\ker\rho$．如果 $m\in M$，则 $m=(m-\rho m)+\rho m$. 显然 $\rho m\in \mathrm{im}\rho=S$. 另一方面，因为 $\rho m\in S$，所以有 $\rho\rho m=\rho m$，从而 $\rho(m-\rho m)=\rho m-\rho\rho m=0$. 所以 $M=S+T$.

如果 $m\in S$，则 $\rho m=m$；如果 $m\in T=\ker\rho$，则 $\rho m=0$. 因此，如果 $m\in S\cap T$，则 $m=0$. 所以 $S\cap T=\{0\}$，从而 $M=S\oplus T$.

关于逆命题，如果 $M=S\oplus T$，则每个 $m\in M$ 有形如 $m=s+t$ 的唯一表达式，其中 $s\in S$ 和 $t\in T$，容易验证由 $\rho: s+t\mapsto s$ 定义的 $\rho: M\to S$ 是收缩 $M\to S$. ■

系 7.18 如果 $M=S\oplus T$ 和 $S\subseteq A\subseteq M$，则 $A=S\oplus(A\cap T)$.

证明 设 $\rho: M\to S$ 是收缩 $s+t\mapsto s$. 因 $S\subseteq A$，限制 $\rho|A: A\to S$ 也是收缩，且 $\ker\rho|A=$

$A \cap T$. ■

直和结构可以扩展到有限个子模．也有内和外两种形式．

定义 设 $S_1, \cdots, S_n$ 是 R-模．定义**外直和**

$$S_1 \sqcup \cdots \sqcup S_n$$

为这样的 R-模，它的底集是笛卡儿积 $S_1 \times \cdots \times S_n$，它的运算是

$$(s_1, \cdots, s_n) + (s_1', \cdots, s_n') = (s_1 + s_1', \cdots, s_n + s_n')$$

$$r(s_1, \cdots, s_n) = (rs_1, \cdots, rs_n).$$

[434]

设 M 是模，并设 $S_1, \cdots, S_n$ 是 M 的子模．如果每个 $m \in M$ 都有唯一的形如 $m = s_1 + \cdots + s_n$ 的表达式，其中对一切 $i = 1, \cdots, n$ 有 $s_i \in S_i$，则定义 M 是**内直和**

$$M = S_1 \oplus \cdots \oplus S_n.$$

当内直和已有定义时，我们留给读者证明此时内和外两种直和同构．

例如，如果 V 是域 k 上的 n 维向量空间，$v_1, \cdots, v_n$ 是一组基，则

$$V = \langle v_1 \rangle \oplus \cdots \oplus \langle v_n \rangle.$$

如果 $S_1, \cdots, S_n$ 是模 M 的子模，什么时候由 S_i 生成的子模 $\langle S_1, \cdots, S_n \rangle$ 等于它们的直和？常犯的错误是认为只要对一切 $i \neq j$ 有 $S_i \cap S_j = \{0\}$ 就够了，但例 5.3 说明这是不够的．

命题 7.19 设 $M = S_1 + \cdots + S_n$，其中 S_i 是子模，即每个 $m \in M$ 有（不必唯一）形如

$$m = s_1 + \cdots + s_n$$

的表达式，其中对一切 i 有 $s_i \in S_i$．则 $M = S_1 \oplus \cdots \oplus S_n$ 当且仅当对每个 i，

$$S_i \cap \langle S_1 + \cdots + \hat{S}_i + \cdots + S_n \rangle = \{0\},$$

其中 $\hat{S}_i$ 表示从和中删去 S_i 这一项．

证明 简单修改命题 5.4 即可．习题 7.79 中将这个命题推广到无限个子模． ■

下面是模字典中的最后一个定义．

定义 称 R-映射和 R-模的序列

$$\cdots \to M_{n+1} \xrightarrow{f_{n+1}} M_n \xrightarrow{f_n} M_{n-1} \to \cdots$$

为**正合列**㊀，如果对一切 n，$\mathrm{im} f_{n+1} = \ker f_n$．

注意，没有必要对箭头 $0 \xrightarrow{f} A$ 或 $B \xrightarrow{g} 0$ 进行标记，因为在两种情形中都只有唯一的映射，就是 $f: 0 \mapsto 0$ 或对一切 $b \in B$，常数同态 $g(b) = 0$．㊁

[435]

下面是一个同态序列是正合列的几个简单推论．

命题 7.20 （ⅰ）序列 $0 \to A \xrightarrow{f} B$ 是正合的当且仅当 f 是单射．

（ⅱ）序列 $B \xrightarrow{g} C \to 0$ 是正合的当且仅当 g 是满射．

（ⅲ）序列 $0 \to A \xrightarrow{h} B \to 0$ 是正合的当且仅当 h 是同构．

㊀ 正合（exact）这个术语来自高等微积分，在那里称一个微分形式 ω 为闭的，如果 $d\omega = 0$，而称之为 exact（恰当的），如果有某个函数 h 使得 $\omega = dh$（见命题 9.146）．这个术语由代数拓扑学家胡雷维奇（W. Hurewicz）创造．看一看 Hurewicz－Wallman 的书《Dimension Theory》是有趣的，该书正好写在这个术语创造之前．我们可以看到使用字 exact 可以使许多陈述变得更简单．

㊁ 在图中，我们常用 0 替代 $\{0\}$．

证明 （ⅰ）$0\to A$ 的象是$\{0\}$，从而正合性给出 $\ker f=\{0\}$，因此 f 是单射．反之，给定 $f: A\to B$，存在正合列 $\ker f\to A\xrightarrow{f}B$．如果 f 是单射，则 $\ker f=\{0\}$．

（ⅱ）$C\to 0$ 的核是 C，从而正合性给出 $\mathrm{im}g=C$，因此 g 是满射．反之，给定 $g: B\to C$，存在正合列 $B\xrightarrow{g}C\to C/\mathrm{im}g$（见习题 7.13)．如果 g 是满射，则 $C=\mathrm{im}g$ 和 $C/\mathrm{im}g=\{0\}$．

（ⅲ）（ⅰ）证明 h 是单射当且仅当 $0\to A\xrightarrow{h}B$ 是正合列，（ⅱ）证明 h 是满射当且仅当 $A\xrightarrow{h}B\to 0$ 是正合列．所以 h 是同构当且仅当序列 $0\to A\xrightarrow{h}B\to 0$ 是正合列． ■

我们可以用正合列的语言重述同构定理．

定义 **短正合列**是指形如

$$0\to A\xrightarrow{f}B\xrightarrow{g}C\to 0$$

的正合列．我们也称这个短正合列为 A 和 C **扩张**．

有些作者把它称作 C 和 A 的扩张，有些作者说中间模 B 是一个扩张．

命题 7.21 （ⅰ）如果 $0\to A\xrightarrow{f}B\xrightarrow{g}C\to 0$ 是短正合列，则

$$A\cong \mathrm{im}f \quad 和 \quad B/\mathrm{im}f\cong C.$$

（ⅱ）如果 $T\subseteq S\subseteq M$ 是子模的塔，则存在正合列

$$0\to S/T\xrightarrow{f}M/T\xrightarrow{g}M/S\to 0.$$

证明 （ⅰ）因 f 是单射，它是同构 $A\to \mathrm{im}f$．第一同构定理给出 $B/\ker g\cong \mathrm{im}g$．然而由正合性，$\ker g=\mathrm{im}f$ 和 $\mathrm{im}g=C$，所以 $B/\mathrm{im}f\cong C$．

（ⅱ）这正是第三同构定理的复述．定义 $f: S/T\to M/T$ 为包含映射，定义 $g: M/T\to M/S$ 为“陪集的扩大”：$g: m+T\mapsto m+S$．和定理 7.10 的证明一样，g 是满射，且 $\ker g=S/T=\mathrm{im}f$． ■

436

在 A 是 B 的子模和 $f: A\to B$ 是包含映射的特殊情形中，$0\to A\xrightarrow{f}B\xrightarrow{g}C\to 0$ 的正合性给出 $B/A\cong C$．

定义 称短正合列

$$0\to A\xrightarrow{i}B\xrightarrow{p}C\to 0$$

分裂，如果存在映射 $j: C\to B$ 使得 $pj=1_C$．

命题 7.22 如果短正合列

$$0\to A\xrightarrow{i}B\xrightarrow{p}C\to 0$$

分裂，则 $B\cong A\sqcup C$．

注 习题 7.17 刻画了分裂短正合列．

证明 我们证明 $B=\mathrm{im}i\oplus \mathrm{im}j$，其中 $j: C\to B$ 满足 $pj=1_C$．如果 $b\in B$，则因 $pj=1_C$，从而 $p(b-jpb)=pb-pj(pb)=0$，由此 $pb\in C$，$b-jpb\in\ker p$．根据正合性，存在 $a\in A$ 使得 $ia=b-jpb$．因此 $B=\mathrm{im}i+\mathrm{im}j$．剩下的是证明 $\mathrm{im}i\cap\mathrm{im}j=\{0\}$．如果 $ia=x=jc$，则因 $pi=0$ 有 $px=pia=0$，而因 $pj=1_C$ 有 $px=pjc=c$．所以 $x=jc=0$，因此 $B\cong A\sqcup C$． ■

上面这个命题的逆命题不成立．设 $A=\langle a\rangle$，$B=\langle b\rangle$ 和 $C=\langle c\rangle$ 是阶分别为 2，4 和 2 的循环群．如果定义 $i: A\to B$ 为 $i(a)=2b$，定义 $p: B\to C$ 为 $p(b)=c$，则 $0\to A\xrightarrow{i}B\xrightarrow{p}C\to 0$ 是正合列，

但不分裂：$\operatorname{im} i = \langle 2b \rangle$ 甚至不是 B 的纯子群．根据习题 7.12，对任意阿贝尔群 M，存在正合列

$$0 \to A \xrightarrow{i'} B \sqcup M \xrightarrow{p'} C \sqcup M \to 0,$$

其中 $i'(a) = (2b, 0)$ 和 $p'(b, m) = (c, m)$，这个序列也不分裂．如果选取 $M = \mathbb{I}_4[x] \sqcup \mathbb{I}_2[x]$（直和项分别是$\mathbb{I}_4$ 上的多项式环和$\mathbb{I}_2$ 上的多项式环），则 $A \sqcup (C \sqcup M) \cong B \sqcup M$.（对熟悉无限直和的读者，$M$ 是 $\mathbb{I}_4 \sqcup \mathbb{I}_2$ 的无限个复制的直和，我们在本章稍后介绍无限直和．）

下面用这个思想来刻画诺特环．

命题 7.23 （i）交换环 R 是诺特环当且仅当有限生成 R-模 M 的每个子模也是有限生成的．

（ii）如果 R 是 PID 且 M 可以由 n 个元素生成，则 M 的每个子模可以由 n 个或少于 n 个元素生成．

437

注 在更一般的情形下，命题7.23(ii)不真．例如，如果 R 不是 PID，则存在某个非主理想的理想 I. 由此，R 可以只有一个生成元，而它的子模 I 不能由一个元素生成．

证明 （i）假定一个有限生成 R-模的每个子模也是有限生成的．特别地，R 是循环R-模，因此是有限生成的，从而它的每个子模也是有限生成的．而 R 的子模是理想，所以每个理想都是有限生成的，即 R 是诺特环．

对 $n \geqslant 1$ 用归纳法证明逆命题，其中 $M = \langle x_1, \cdots, x_n \rangle$. 如果 $n=1$，则 M 是循环的，因此命题 7.12 给出某个理想 I 使得 $M \cong R/I$. 如果 $S \subseteq M$，则对应定理给出理想 J 使得 $I \subseteq J \subseteq R$ 和 $S \cong J/I$. 而 R 是诺特环，从而 J 是有限生成的，因此 J/I 也是有限生成的．

如果 $n \geqslant 1$ 和 $M = \langle x_1, \cdots, x_n, x_{n+1} \rangle$，考虑正合列

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0,$$

其中 $M' = \langle x_1, \cdots, x_n \rangle, M'' = M/M'$，$i$ 是包含映射，p 是自然映射．注意 M'' 是循环的，它由 $x_{n+1} + M'$ 生成．如果 $S \subseteq M$ 是子模，则有正合列

$$0 \to S \cap M' \to S \to S/(S \cap M') \to 0.$$

现在 $S \cap M' \subseteq M'$，因此根据归纳假设，它是有限生成的．又，$S/(S \cap M') \cong (S+M')/M' \subseteq M/M'$，因此根据基础步，$S/(S \cap M')$ 是有限生成的．用习题 7.15 可推出 S 是有限生成的．

（ii）对 $n \geqslant 1$ 用归纳法证明该陈述．如果 M 是循环的，则 $M \cong R/I$. 如果 $S \subseteq M$，则有 R 中某个包含 I 的理想 J 使得 $S \cong J/I$. 因 R 是 PID，所以 J 是主理想，因此 J/I 是循环的．

关于归纳步，我们参看（i）中的正合列

$$0 \to S \cap M' \to S \to S/(S \cap M') \to 0,$$

其中 $M = \langle x_1, \cdots, x_n, x_{n+1} \rangle$ 和 $M' = \langle x_1, \cdots, x_n \rangle$. 由归纳假设，$S \cap M'$ 可以被 n 个或少于 n 个元素生成，而基础步表明 $S/(S \cap M')$ 是循环的，习题 7.15 证明 S 可以被 $n+1$ 个或少于 $n+1$ 个元素生成． ■

用命题7.23(ii)证明的下一命题表明代数整数的和与积也是代数整数．如果 α 和 β 是代数整数，不难给出以 $\alpha + \beta$ 和 $\alpha\beta$ 为根的首一多项式，但是求全部系数在$\mathbb{Z}$中的这样的多项式就得做一点工作（见 Pollard 所著的《The Theory of Algebraic Numbers》，33 页）．

命题 7.24 设 $\alpha \in \mathbb{C}$，定义 $\mathbb{Z}[\alpha] = \{g(\alpha) : g(x) \in \mathbb{Z}[x]\}$.

（i）$\mathbb{Z}[\alpha]$ 是$\mathbb{C}$ 的子环．

438

（ii）复数 α 是代数整数当且仅当$\mathbb{Z}[\alpha]$ 是有限生成的加法阿贝尔群．

（iii）一切代数整数的集合是$\mathbb{C}$ 的子环．

证明 （i）取 $g(x) = 1$ 是常数多项式，则 $1 = g(\alpha)$，从而有 $1 \in \mathbb{Z}[\alpha]$. 如果 $f(\alpha), g(\alpha) \in \mathbb{Z}[\alpha]$，则 $f(\alpha) + g(\alpha) = h(\alpha)$ 也在$\mathbb{Z}[\alpha]$中，其中 $h(x) = f(x) + g(x)$. 同样，$f(\alpha)g(\alpha) \in \mathbb{Z}[\alpha]$，因此$\mathbb{Z}[\alpha]$是$\mathbb{C}$的子环.

(ⅱ) 如果α是代数整数，则存在首一多项式$f(x) \in \mathbb{Z}[x]$以α为根．我们断言，如果$\deg(f) = n$，则$\mathbb{Z}[\alpha] = G$，其中G是满足$m_i \in \mathbb{Z}$的一切线性组合$m_0 + m_1\alpha + \cdots + m_{n-1}\alpha^{n-1}$的集合．显然$G \subseteq \mathbb{Z}[\alpha]$. 关于反包含，每个元素$u \in \mathbb{Z}[\alpha]$都形如$u = g(\alpha)$，其中$g(x) \in \mathbb{Z}[x]$. 因$f(x)$是首一的，带余除法（系 3.22）给出$q(x), r(x) \in \mathbb{Z}[x]$使得$g(x) = q(x)f(x) + r(x)$，其中$r(x) = 0$或$\deg(r) < \deg(f) = n$．所以，

$$u = g(\alpha) = q(\alpha)f(\alpha) + r(\alpha) = r(\alpha) \in G.$$

由此，加法群$\mathbb{Z}[\alpha]$是有限生成的．

反之，如果交换环$\mathbb{Z}[\alpha]$的加法群是有限生成的，即$\mathbb{Z}[\alpha] = \langle g_1, \cdots, g_m \rangle$是阿贝尔群，则每个$g_j$都是$\alpha$的幂的$\mathbb{Z}$-线性组合．设$m$是出现在这些$g$中的$\alpha$的最大幂．因$\mathbb{Z}[\alpha]$是交换环，$\alpha^{m+1} \in \mathbb{Z}[\alpha]$，从而$\alpha^{m+1}$可以表示为$\alpha$的较小幂的$\mathbb{Z}$-线性组合，比如$\alpha^{m+1} = \sum_{i=0}^{m} b_i\alpha^i$，其中$b_i \in \mathbb{Z}$．所以$\alpha$是$f(x) = x^{m+1} - \sum_{i=0}^{m} b_i x^i$的根，$f(x)$是$\mathbb{Z}[x]$中的首一多项式，因此$\alpha$是代数整数．

(ⅲ) 假设α和β是代数整数，设α是次数为n的首一多项式$f(x) \in \mathbb{Z}[x]$的根，β是次数为m的首一多项式$g(x) \in \mathbb{Z}[x]$的根．现在$\mathbb{Z}[\alpha\beta]$是$G = \langle \alpha^i\beta^j : 0 \leqslant i < n, 0 \leqslant j < m \rangle$的加法子群．因$G$是有限生成的，从而根据命题 7.23(ⅱ)，它的子群$\mathbb{Z}[\alpha\beta]$也是有限生成的，因此$\alpha\beta$是代数整数．同样，$\mathbb{Z}[\alpha + \beta]$是$\langle \alpha^i\beta^j : i + j \leqslant n + m - 1 \rangle$的加法子群，因此$\alpha + \beta$也是代数整数． ■

上面的定理给出了证明整数a是整数b的因数的一种方法．如果能证明b/a是代数整数，则因为b/a显然是有理数，它必是整数．事实上在第8章中，将用它来证明有限群G的不可约特征标的次数是$|G|$的因数．

习题

7.1 设R是交换环．（加法）阿贝尔群M称为**殆R-模**，如果存在函数$R \times M \to M$满足R-模的除了公理（ⅳ）的一切公理：我们不假定对一切$m \in M$有$1m = m$．

证明

439

$$M = M_1 \oplus M_0,$$

其中

$$M_1 = \{m \in M : 1m = m\} \text{ 和 } M_0 = \{m \in M: \text{对一切 } r \in R \text{ 有 } rm = 0\}$$

是M的子群，它们是殆R-模，事实上，M_1是R-模．

7.2 如果X是模M的子集，证明由X生成的M的子模$\langle X \rangle$等于$\bigcap S$，其中交遍历一切包含X的子模$S \subseteq M$.

7.3 证明：如果$f: M \to N$是R-映射，且K是满足$K \subseteq \ker f$的M的子模，则f由$\overline{f}: m + K \mapsto f(m)$诱导出一个$R$-映射$\overline{f}: M/K \to N$.

7.4 设R是交换环，并设J是R中的理想．回忆如果M是一个R-模，则$JM = \{\sum_i j_i m_i : j_i \in J \text{ 和 } m_i \in M\}$是$M$的子模．证明：如果定义标量乘法：

$$(r + J)(m + JM) = rm + JM,$$

则M/JM是R/J-模．由此推出，如果$JM = \{0\}$，则M本身是一个R/J-模，特别地，如果J是R中的极大理想且$JM = \{0\}$，则M是R/J上的向量空间．

7.5 证明对每个R-模M，$\varphi_M: f \mapsto f(1)$给出一个$R$-同构

$$\varphi_M: \mathrm{Hom}_R(R, M) \to M.$$

7.6 设 $F=\sum_{i=1}^{n}\langle b_i\rangle$ 是 R-模的直和，其中由 $r\mapsto rb_i$ 给出的 $f_i: R\to\langle b_i\rangle$ 是同构．证明：如果 M 是 R 中的极大理想，则陪集 $\{b_i+MF: i=1,\cdots,n\}$ 形成域 R/M 上向量空间 F/MF 的基．(见习题 7.4.)

7.7 设 R 和 S 都是交换环，并设 $\varphi: R\to S$ 是环同态．如果 M 是 S-模，证明：如果对一切 $r\in R$ 和 $m\in M$ 定义

$$rm=\varphi(r)m,$$

则 M 也是 R-模．

7.8 设 $M=S_1\sqcup\cdots\sqcup S_n$ 是 R-模的直和．如果对一切 i，$T_i\subseteq S_i$，证明

$$(S_1\sqcup\cdots\sqcup S_n)/(T_1\sqcup\cdots\sqcup T_n)\cong(S_1/T_1)\sqcup\cdots\sqcup(S_n/T_n).$$

7.9 设 R 是交换环，并设 M 是非零 R-模．如果 $m\in M$，定义 $\mathrm{ord}(m)=\{r\in R: rm=0\}$，并定义 $\mathcal{F}=\{\mathrm{ord}(m): m\in M$ 且 $m\neq 0\}$. 证明 $\mathcal{F}$ 中的每个极大元素都是一个素理想．

7.10 设 $A\xrightarrow{f}B\xrightarrow{g}C$ 是模映射的序列．证明 $gf=0$ 当且仅当 $\mathrm{im}f\subseteq\ker g$. 举出一个不是正合的这种序列的例子.

7.11 如果 $0\to M\to 0$ 是正合列，证明 $M=\{0\}$．

7.12 设 $0\to A\to B\to C\to 0$ 是模的短正合列．如果 M 是任意模，证明存在正合列

$$0\to A\oplus M\to B\oplus M\to C\to 0$$

和

$$0\to A\to B\oplus M\to C\oplus M\to 0.$$

440

定义：如果 $f: M\to N$ 是映射，它的**余核**记为 $\mathrm{coker}f$，定义为

$$\mathrm{coker}f=N/\mathrm{im}f.$$

7.13 (i) 证明映射 $f: M\to N$ 是满射当且仅当 $\mathrm{coker}f=\{0\}$．

(ii) 如果 $f: M\to N$ 是映射，证明存在正合列

$$0\to\ker f\to M\xrightarrow{f}N\to\mathrm{coker}f\to 0.$$

7.14 如果 $A\xrightarrow{f}B\to C\xrightarrow{h}D$ 是正合列，证明 f 是满射当且仅当 h 是单射．

7.15 设 $0\to A\xrightarrow{i}B\xrightarrow{p}C\to 0$ 是短正合列．

(i) 假定 $A=\langle X\rangle$ 和 $C=\langle Y\rangle$. 对每个 $y\in Y$，选取 $y'\in B$ 满足 $p(y')=y$. 证明

$$B=\langle i(X)\cup\{y': y\in Y\}\rangle.$$

(ii) 证明：如果 A 和 C 都是有限生成的，则 B 也是有限生成的．更精确地说，如果 A 可以由 m 个元素生成，C 可以由 n 个元素生成，则 B 可以由 $m+n$ 个元素生成．

7.16 证明向量空间的每个短正合列分裂．

7.17 证明短正合列

$$0\to A\xrightarrow{i}B\xrightarrow{p}C\to 0$$

分裂当且仅当存在 $q: B\to A$ 使得 $qi=1_A$．

7.18 (i) 证明映射 $\varphi: B\to C$ 是单射当且仅当 φ 可以左消去，即对一切模 A 和一切映射 $f, g: A\to B$，有 $\varphi f=\varphi g$ 蕴涵 $f=g$.

$$A\underset{g}{\overset{f}{\rightrightarrows}}B\xrightarrow{\varphi}C$$

(ii) 证明 R-映射 $\varphi: B\to C$ 是满射当且仅当 φ 可以右消去，即对一切 R-模 D 和一切 R-映射 $h, k: C\to$

D，有 $h\varphi=k\varphi$ 蕴涵 $h=k$.

$$B \xrightarrow{\varphi} C \underset{k}{\overset{h}{\rightrightarrows}} D$$

7.19 (Eilenberg - Moore) 设 G 是群(可以是非阿贝尔的).

(i) 如果 H 是群 G 的真子群，证明存在群 L 和不同的同态 f，$g: G\to L$ 使得 $f\mid H=g\mid H$.

提示：定义 $L=S_X$，其中 X 表示 H 在 G 中的一切左陪集的族再附加一个元素(记为 ∞). 如果 $a\in G$，定义 $f(a)=f_a\in S_X$ 为 $f_a(\infty)=\infty$ 和 $f_a(bH)=abH$. 定义 $g: G\to S_X$ 为 $g=\gamma\circ f$，其中 $\gamma\in S_X$ 是用对换(H,∞)形成的共轭.

(ii) 如果 A 和 G 是群，证明同态 $\varphi: A\to G$ 是满射当且仅当 φ 可以右消去，即对一切群 L 和一切映射 $f,g: G\to L$，有 $f\varphi=g\varphi$ 蕴涵 $f=g$.

$$B \xrightarrow{\varphi} G \underset{g}{\overset{f}{\rightrightarrows}} L$$

441

7.2 范畴

想象把集合论的原始术语集合和元素换成集合和函数，该怎样定义双射、笛卡儿积、并和交？范畴论将迫使我们用这种方式思考问题．范畴是讨论诸如群、环、向量空间、模、集合和拓扑空间等系统，以及它们各自的变换：同态、函数和连续映射等的一般性质的语言．研究范畴有两个基本理由：一是需要定义函子和自然变换（我们在下一节做这件事），二是范畴迫使我们不是孤立地对待像模这样的对象，而把它放在和一切其他模的相互关系中考虑它（例如我们要作为泛映射问题的解来定义某种模）．

集合论有一个的著名“悖论”，如果我们不注意如何运用不加定义的术语集合和元素，矛盾便会产生．例如，罗素悖论表明如果把每个集团都当作一个集合，我们将陷入怎样的困境．定义**罗素集**为这样的集合 S，它本身不是 S 的成员，即 $S\notin S$. 如果 R 是一切罗素集的族，那么 R 是罗素集吗？一方面，如果 $R\in R$，则 R 不是罗素集. 因为只有罗素集是 R 的成员，我们必有 $R\notin R$，这是一个矛盾．另一方面，如果假定 $R\notin R$，则 R 是罗素集，所以它属于 R（R 包含每个罗素集），又是一个矛盾. 由此得知，必须对什么样的集团可以作为集合提出某些条件（对从属关系 $\in$ 也要提出某些条件）. 避免这个问题的一种方法是考虑用类作为原始术语代替集合使集合论公理化．公理给出有限类和 $\mathbb{N}$ 的存在性；也提出了从给定类构造特定类的法则，按照这些法则构造出来的类称为**集合**．可以定义基数，有一个定理：类是集合当且仅当它是“小的”；即它有一个基数．定义**真类**为不是集合的类．例如 $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ 和 $\mathbb{C}$ 都是集合，而一切集合的集团是真类．颁布某些法则只能应用于集合而不能应用于真类，从而可以避免出现悖论．

定义 一个**范畴** $\mathcal{C}$ 由三个要素组成：**对象**的一个类 $\mathrm{obj}(\mathcal{C})$，对每个有序对象对$(A,B)$的**态射** $\mathrm{Hom}(A,B)$ 的集合，对每个有序三对象组 A,B,C 的**复合** $\mathrm{Hom}(A,B)\times\mathrm{Hom}(B,C)\to\mathrm{Hom}(A,C)$，记为

$$(f,g)\mapsto gf.$$

[我们常用 $f: A\to B$ 或 $A\xrightarrow{f}B$ 表示 $f\in\mathrm{Hom}(A,B)$.] 这些要素受到下面公理的制约：

442

(i) Hom 集合是两两不相交的，[⊖] 即每个态射有唯一的定义域和唯一的目标域.

(ii) 对每个对象 A，有一个**单位态射** $1_A\in\mathrm{Hom}(A,A)$ 满足

⊖ 可以用 ${}_Af_B$ 标记 $f\in\mathrm{Hom}(A,B)$ 以保证两两不相交性.

$$对一切\ f: A \to B, f1_A = f 和 1_B f = f.$$

（iii）复合是结合的：给定态射

$$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D,$$

则

$$h(gf) = (hg)f.$$

在这个思想氛围中，重要的概念不是范畴而是函子，函子将在下一节中引入．但范畴是必需的，因为它们是定义函子的基本要素．类似的情形发生在线性代数中：线性变换是重要概念，但为了定义它我们必须先考虑向量空间．

下面的例子说明定义范畴的某些好处．

例 7.25 （i）$\mathcal{C}$=**集合**．

这个范畴中的对象是集合（不是真类），态射是函数，复合是通常的函数复合．

集合论的一个常用结果是：如果 A 和 B 是集合，则从 A 到 B 的一切函数的类 Hom(A,B)是一个集合．Hom 集两两不相交就是第 1 章中给出的函数相等定义的反映：要使两个函数相等，首先它们要有相同的定义域和相同的目标域（当然，还必须有相同的图像）．

（ii）$\mathcal{C}$ = **群**．

这里的对象是群，态射是同态，复合是通常的复合（同态是函数）．

（iii）$\mathcal{C}$ = **交换环**．

这里的对象是交换环，态射是环同态，复合是通常的复合．

（iv）$\mathcal{C} = {}_R\mathbf{Mod}$.㊀

这个范畴中的对象是 R-模，其中 R 是交换环，态射是 R- 同态，复合是通常的复合．我们记 ${}_R\mathbf{Mod}$ 中的 Hom(A,B) 为

$$\mathrm{Hom}_R(A,B).$$

如果 $R = \mathbb{Z}$，我们常写

$$_{\mathbb{Z}}\mathbf{Mod} = \mathbf{Ab}$$

用以提醒自己 $\mathbb{Z}$-模就是阿贝尔群．

443

（v）$\mathcal{C}$ = **PO**(X).

如果 X 是一个偏序集，可以把它看作一个范畴，其对象是 X 的元素，Hom 集或者是空集或者只有一个元素：

$$\mathrm{Hom}(x,\ y) = \begin{cases} \varnothing & 如果\ x \not\preceq y \\ \{\kappa_y^x\} & 如果\ x \preceq y \end{cases}$$

（符号 κ_y^x 表示当 $x \preceq y$ 时在 Hom 集中的唯一元素），复合由

$$\kappa_z^y \kappa_y^x = \kappa_z^x$$

给出．注意由自反性，$1_x = \kappa_x^x$，因 $\preceq$ 是传递的，所以复合有意义．㊁

在范畴的定义中，我们强调 Hom(A,B) 是一个集合，但没有排除它是空集的可能性．范畴

㊀ 在第 8 章中引入非交换环之后，我们记左 R-模的范畴为${}_R\mathbf{Mod}$，而记右 R-模的范畴为 $\mathbf{Mod}_R$．

㊁ 称非空集合 X 为**拟序集**，如果有自反和传递的关系 $x \preceq y$（如果这个关系还是反对称的，则 X 是偏序集）．对每个拟序集，**PO**(X)是范畴．

PO(X)的例子中这种可能性就出现了．[在一个范畴$\mathcal{C}$中不是每个 Hom 集都可能空，因为对每个对象 $A \in \mathcal{C}$，$\mathrm{Hom}(A,A)$ 中包含单位态射 1_A，所以 $\mathrm{Hom}(A,A) \neq \varnothing$.]

(vi) $\mathcal{C} = \mathcal{C}(G)$.

如果 G 是群，则下面的描述定义范畴 $\mathcal{C}(G)$：它只有一个对象记为 $*$，$\mathrm{Hom}(*,*) = G$，复合

$$\mathrm{Hom}(*,*) \times \mathrm{Hom}(*,*) \to \mathrm{Hom}(*,*);$$

即 $G \times G \to G$ 是 G 中 给定的乘法．公理验证留给读者.㊀

范畴$\mathcal{C}(G)$有一个不常有的性质．因 $*$ 仅仅是一个对象而不是集合，因此没有函数 $* \to *$ 可以定义在它上面；于是这里的态射不是函数．这个范畴的另一个古怪的性质是从只有一个对象得出的另一个推论：这里没有真子对象．

(vii) 有许多有趣的非代数的范畴的例子．例如 $\mathcal{C} =$ **Top**，这个范畴的对象是一切拓扑空间，态射是一切连续函数，复合是通常的复合． ■

下面是如何把同构翻译为范畴的语言．

定义 称范畴$\mathcal{C}$中的态射 $f: A \to B$ 为**等价**(或**同构**)，如果存在$\mathcal{C}$中的态射 $g: B \to A$ 使得

$$gf = 1_A \text{ 和 } fg = 1_B.$$

444 称态射 g 为 f 的**逆**．

易知等价的逆是唯一的．

范畴中的单位态射恒为等价．如果 $\mathcal{C} =$ **PO**(X)，其中 X 是偏序集，则唯一的一个等价是单位态射；如果 $\mathcal{C} = \mathcal{C}(G)$，其中 G 是群（见例7.25(vi)），则每个态射都是等价；如果 $\mathcal{C} =$ **集合**，则等价是双射；如果 $\mathcal{C} =$ **群**，$\mathcal{C} = {}_R$**Mod**，或 $\mathcal{C} =$ **交换环**，则等价是同构；如果 $\mathcal{C} =$ **Top**，则等价是同胚．

我们给范畴${}_R$**Mod** 的一个特性定一个名称（在命题 7.5 中看到的），这个特性就是同态可加，它不是一般范畴所共有的．

定义 称范畴$\mathcal{C}$为**预加性**的，如果每个 $\mathrm{Hom}(A,B)$ 配置有二元运算使它变成一个（加法）阿贝尔群，且对这个运算分配律成立：对一切 $f,g \in \mathrm{Hom}(A,B)$，

(i) 如果 $p: B \to B'$，则

$$p(f+g) = pf + pg \in \mathrm{Hom}(A,B');$$

(ii) 如果 $q: A' \to A$，则

$$(f+g)q = fq + gq \in \mathrm{Hom}(A',B).$$

习题 7.22 中证明群范畴不具备预加性范畴的结构．

范畴是用对象和态射的术语定义的，它的对象不必是集合，它的态射不必是函数 [在例7.25(vi)中$\mathcal{C}(G)$就是这样的范畴]．我们现在尝试在集合范畴和 ${}_R$**Mod** 范畴中描述各种结构，这些结构在任意范畴中也有意义.

在命题7.15(iii)中我们给出直 和 $M = A \oplus B$ 的刻画：存在同态 $p: M \to A, q: M \to B, i: A \to M$ 和 $j: B \to M$ 使得

$$pi = 1_A, qj = 1_B, pj = 0, qi = 0 \text{ 和 } ip + jq = 1_M.$$

即使直和的这个描述是用箭头的语言实现的，但要使得它在每个范畴中都有意义，还不够一般化，它用到${}_R$**Mod** 范畴的一个性质，而集合范畴不具备这个性质，例如态射可加．

在系 7.17 中，我们用箭头给出直和的另一种描述：

㊀ 证明 $\mathcal{C}(G)$ 是范畴时，不必要求 G 中每个元素都有逆，因此对每个幺半群 G，$\mathcal{C}(G)$ 也是范畴．

存在映射 $\rho: M \to S$ 使得 $\rho s = s$；此外，$\ker\rho = \operatorname{im} j$，$\operatorname{im}\rho = \operatorname{im} i$，对每个 $s \in \operatorname{im}\rho$，$\rho(s) = s$．这个描述在集合中也有意义，但在任意范畴中不是都有意义的，因为不能定义态射的象．例如$\mathcal{C}(G)$中的态射［见例7.25(ⅵ)］是 $\mathrm{Hom}(*,*)=G$ 中的元素而不是函数，因此态射的象没有明确的意义．

然而，我们可以用范畴语言定义直和项：称对象 S 是（等价于）对象 M 的收缩核，如果存在态射

$$i: S \to M \text{ 和 } p: M \to S$$

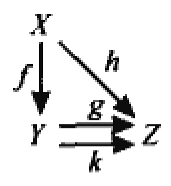
满足 $pi = 1_S$． [445]

用范畴方式思考的一个好处是使得我们看到以前没有认识的相似性．例如，我们将立刻看到在${}_R\mathbf{Mod}$ 范畴中的直和和集合范畴中的不相交并是同一概念．

我们从一个十分形式化的定义开始．

定义 *范畴$\mathcal{C}$中的一个***图***是指一个有向多重图*[⊖]*，它的顶点是$\mathcal{C}$中的对象，它的箭头是$\mathcal{C}$中的态射．*

例如，



是范畴中的图，

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle g'}\downarrow & & \downarrow{\scriptstyle g} \\ C & \xrightarrow[f']{} & D \end{array}$$

也是范畴中的图．如果把箭头想象为“单行道”，则图中的一条路径就是从一个顶点“走到”另一个顶点，但注意不要走错路．图中的一条路径可以看作态射的复合．

定义 *称图***交换***，如果对每个顶点对 A 和 B，从 A 到 B 的任意两条路径相等；即复合是相同的态射．*

例如，如果 $gf = h, kf = h$ 则上面的三角形图交换．如果 $gf = f'g'$，则上面的正方形图交换．这里所用的交换这个术语就来自这个例子．

如果 A 和 B 是集合 S 的子集，则它们的交定义为：

$$A \cap B = \{s \in S : s \in A \text{ 和 } s \in B\}$$

（如果两个集合不是作为子集给出的，则它们的交或许不是我们所期望的：例如，如果$\mathbb{Q}$定义为整数有序对 (m,n) 的一切等价类，其中 $n \neq 0$，则$\mathbb{Z} \cap \mathbb{Q} = \varnothing$）．

我们可以通过“分离”两个重叠的子集 A，B 迫使它们变成不相交的．考虑笛卡儿积 $(A \cup B) \times \{1,2\}$，并考虑子集 $A' = A \times \{1\}$ 和 $B' = B \times \{2\}$．显然 $A' \cap B' = \varnothing$，这是因为交中的一个点必有坐标 $(a,1) = (b,2)$，这是不可能的，因为它们的第二个坐标不等．称 $A' \cup B'$ 为A,B的**不相交并**．注意由 $\alpha: a \mapsto (a,1)$ 和 $\beta: b \mapsto (b,2)$ 给出的函数 $\alpha: A \to A'$ 和 $\beta: B \to B'$．记不相交并 $A' \cup B'$ 为 $A \sqcup B$． [446]

如果对某个集合 X 有函数 $f: A \to X$ 和 $g: B \to X$，则存在唯一的函数 $h: A \sqcup B \to X$，它由

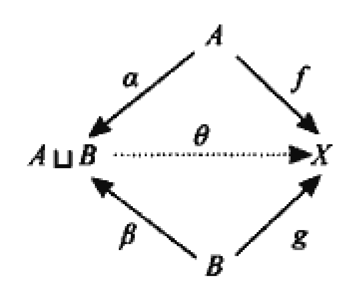
$$h(u) = \begin{cases} f(u) & \text{如果 } u \in A \\ g(u) & \text{如果 } u \in B \end{cases}$$

⊖ 有向多重图由称为顶点的一个集合 V 以及对每个有序对 $(u,v) \in V \times V$ 的一个称为u 到v 的箭头的集合（可以是空集）$\mathrm{arr}(u,v)$ 组成．

给出．因 A，B 是不相交的，所以函数 h 是合理定义的．

下面是用范畴方式（即用图）描述这个构造．

定义 如果 A，B 是范畴$\mathcal{C}$中的对象，则它们的**余积**（记为 $A\sqcup B$）是指 $\mathrm{obj}(\mathcal{C})$ 中的一个对象C连同**内射态射** $\alpha: A\to A\sqcup B$ 和 $\beta\to A\sqcup B$ 满足对$\mathcal{C}$中每个对象 X 和每对态射 $f: A\to X, g: B\to X$，存在唯一的态射 $\theta: A\sqcup B\to X$ 使得下图交换（即 $\theta\alpha=f,\theta\beta=g$）．



这里是对刚构造的集合 $A\sqcup B = A'\cup B'\subseteq (A\cup B)\times\{1,2\}$ 正式证明它是集合范畴中的余积．如果 X 是任意集合，$f: A\to X$ 和 $g: B\to X$ 是任意给定的函数，则存在函数 $\theta: A\sqcup B\to X$ 同时扩张 f 和 g．如果 $c\in A\sqcup B$，则 $c=(a,1)\in A'$ 或 $c=(b,2)\in B'$．定义 $\theta((a,1))=f(a),\theta((b,2))=g(b)$，由此 $\theta\alpha=f,\theta\beta=g$．我们证明 θ 是 $A\sqcup B$ 上唯一的函数同时扩张了 f 和 g．如果$\psi: A\sqcup B\to X$ 满足$\psi\alpha=f,\psi\beta=g$，则

$$\psi(\alpha(a))=\psi((a,1))=f(a)=\theta((a,1)).$$

同样，

$$\psi((b,2))=g(b).$$

所以 ψ和 θ 在 $A'\cup B'=A\sqcup B$ 上一致，从而$\psi=\theta$．

我们没有声称余积恒存在，事实上，容易构造范畴的例子使得其中有一对对象没有余积（见习题 7.21）．然而我们的论证表明在集合范畴中余积确实存在，在那里余积是不相交并．在群范畴中余积也存在，它们称为**自由积**，自由群是无限循环群的自由积（类似于自由阿贝尔群是无限循环群的直和）．库洛什（A. G. Kurosh）的一个定理说自由积的每个子群本身是自由积．

447

命题 7.26 如果 A,B 是 R-模，则它们在${}_R\mathbf{Mod}$ 范畴中的余积存在，它就是直和 $C=A\sqcup B$．

证明 命题的陈述并不完全，因为余积需要内射态射 α 和 β．$C=A\sqcup B$ 的底集是笛卡儿积 $A\times B$，因此可以定义 $\alpha: A\to C$ 为 $\alpha: a\mapsto(a,0)$，定义 $\beta: B\to C$ 为 $\beta: b\mapsto(0,b)$．

现在设 X 是模，并设 $f: A\to X$，$g: B\to X$ 是同态．定义 $\theta: C\to X$ 为 $\theta: (a,b)\mapsto f(a)+g(b)$．首先，图交换：如果 $a\in A$，则 $\theta\alpha(a)=\theta((a,0))=f(a)$，同样，如果 $b\in B$，则 $\theta\beta(b)=\theta((0,b))=g(b)$．最后，$\theta$ 是唯一的．如果ψ：$C\to X$ 使得图交换，则对一切 $a\in A,\psi((a,0))=f(a)$，对一切 $b\in B$，$\psi((0,b))=g(b)$．因ψ 是同态，我们有

$$\begin{aligned}\psi((a,b))&=\psi((a,0)+(0,b))\\&=\psi((a,0))+\psi((0,b))=f(a)+g(b).\end{aligned}$$

所以，$\psi=\theta$． ■

我们给出命题 7.26 证明中的映射 θ 的一个明确的公式．如果 $f: A\to X$，$g: B\to X$ 是给定的同态，则 $\theta: A\oplus B\to X$ 由

$$\theta: (a,b)\mapsto f(a)+g(b)$$

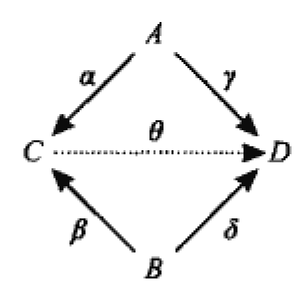
给出．

下一命题的证明要点经常用到；在引理 5.74 中证明非阿贝尔自由群的秩是合理定义的时候已经

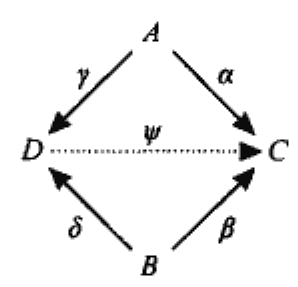
看到过.

命题 7.27 如果$\mathcal{C}$是范畴，A,B是$\mathcal{C}$中的对象，则A,B的任意两个余积如果存在的话必等价.

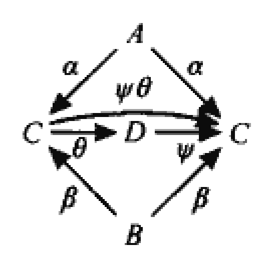
证明 假设C，D是A，B的两个余积．更详细地说，假定$\alpha: A\to C,\beta: B\to C,\gamma: A\to D,\delta: B\to D$是内射态射．如果在定义$C$的图中取$X=D$，则存在态射$\theta: C\to D$使得下图交换.



同样，如果在定义D的图中，取$X=C$，我们得到态射$\psi: D\to C$使得下图交换. 448



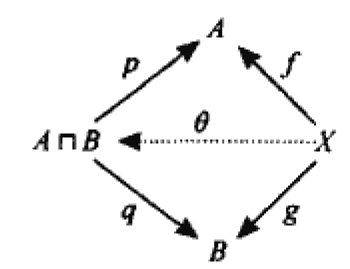
现在考虑下面的图，它是由这两个图连接起来形成的.



因为$\psi\theta\alpha=\psi\gamma=\alpha$，$\psi\theta\beta=\psi\delta=\beta$，这个图交换．显然，恒等态射$1_C: C\to C$也使得这个图交换．由于定义余积的图中虚线箭头是唯一的，所以$\psi\theta=1_C$．作必要的修改后，同样的论证可以证明$\theta\psi=1_D$．由此可知$\theta: C\to D$是等价. ■

非正式地说，称范畴$\mathcal{C}$中的一个对象S为**泛映射问题**的一个**解**，如果它是由一个图来定义的，在这个图中，一旦变更一个对象X和多个态射，便存在唯一态射使得新图交换."元理论"是如果解存在，则不计等价解唯一．刚才给出的证明是证明元理论的原型(如果我们认真起来，则元理论的陈述可以更精确，然后可以证明它，见习题 7.29；关于相应的定义、陈述和证明见 Mac Lane 所著的《Categories for the Working Mathematician》第3章)．证明分两步，第一，如果C，D都是解，则在表明C是解的对应图中令$X=D$得态射$\theta: C\to D$，在表明D是解的对应图中令$X=C$得态射$\psi: D\to C$．第二，在关于C的图中令$X=C$并证明$\psi\theta$和1_C都是使得图交换的"虚线"态射；由于这样的虚线态射是唯一的，从而$\psi\theta=1_C$．同样，另一个复合$\theta\psi=1_D$，因此θ是等价.

定义 如果A,B是范畴$\mathcal{C}$中的对象，则它们的**积**(记为$A\sqcap B$)是对象$P\in\mathcal{C}$和态射$p: P\to A$，$q: P\to B$使得对每个对象$X\in\mathcal{C}$和每对态射$f: X\to A$，$g: X\to B$，存在唯一的态射$\theta: X\to P$使得下图交换： 449



两个集合 A 和 B 的笛卡儿积 $P = A\times B$ 是集合范畴中的范畴积．定义 $p: A\times B\to A$ 为 $p:(a,b)\mapsto a$，定义 $q: A\times B\to B$ 为 $q:(a,b)\mapsto b$. 如果 X 是集合，$f: X\to A, g: X\to B$ 是函数，则读者可以证明由 $\theta: x\mapsto(f(x),g(x))\in A\times B$ 定义的 $\theta: X\to A\times B$ 满足必需的条件．

命题 7.28 如果 A,B 是范畴$\mathcal{C}$中的对象，则 A 和 B 的任意两个积如果存在必等价．

证明 修改证明的原型，即命题 7.27 的证明． ■

读者需注意，反转定义余积的图中的一切箭头得到定义积的图．在习题 7.18 中可以看到类似的反转箭头：在 ${}_R\mathbf{Mod}$ 范畴中，反转刻画单射的图中的一切箭头得到刻画满射的图．如果 S 是由图 $\mathcal{D}$ 提出的泛映射问题的一个解，令 $\mathcal{D}'$ 是反转$\mathcal{D}$ 中一切箭头而得的图．如果 S' 是由$\mathcal{D}'$ 提出的泛映射问题的一个解，则称 S 和 S' **对偶**．有范畴的例子，其中一个对象和它的对偶对象都存在，也有一个对象存在而它的对偶不存在的例子．

两个模的积是什么？

命题 7.29 如果 R 是交换环，A，B 是 R-模，则存在它们的（范畴）积 $A\sqcap B$，事实上，

$$A\sqcap B\cong A\sqcup B.$$

注 由此，两个对象的积和余积虽然在集合范畴中不同，但在 ${}_R\mathbf{Mod}$ 范畴中相同．

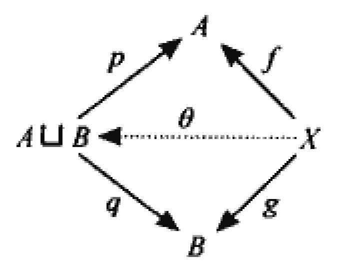
证明 在命题7.15(iii)中，我们用满足等式

$$pi = 1_A, qj = 1_B, pj = 0, qi = 0 \text{ 和 } ip + jq = 1_M$$

的投射和内射态射

$$A \underset{p}{\overset{i}{\rightleftarrows}} M \underset{j}{\overset{q}{\leftrightarrows}} B$$

[450] 的存在性刻画了 $M\cong A\sqcup B$. 如果 X 是模，$f: X\to A, g: X\to B$ 是同态，定义 $\theta: X\to A\sqcup B$ 为$\theta(x) = if(x)+jg(x)$．积的图



交换，这是因为对一切 $x\in X$，

$$p\theta(x) = pif(x)+pjg(x) = pif(x) = f(x)$$

（用给定的等式），且同样有 $q\theta(x) = g(x)$. 为证明 θ 的唯一性，注意等式 $ip+jq = 1_{A\sqcup B}$ 给出

$$\psi = ip\psi + jq\psi = if + jg = \theta. \quad ■$$

习题 7.23 证明了在群范畴中直积是积．

有（至少）两种方法把模的直和的概念从两个直和项推广到直和项的加标族．

定义 设 R 是交换环，$\{A_i: i\in I\}$ 是一个 R-模的加标族．**直积** $\prod_{i\in I} A_i$ 是指笛卡儿积［即对一切 i，第 i 个坐标 a_i 在 A_i 中的一切 I 元组[⊖]］连同坐标状态的加法和标量乘法：

$$(a_i)+(b_i) = (a_i+b_i)$$
$$r(a_i) = (ra_i),$$

⊖ I 元组是函数 $f: I\to\bigcup_i A_i$，其中对一切 $i\in I, f(i)\in A_i$．

其中 $r\in R$，以及对一切 $i, a_i, b_i \in A_i$.

直和是指由只有有限个非零坐标的一切 (a_i) 组成的 $\prod_{i\in I} A_i$ 的子模，记为 $\sum_{i\in I} A_i$（也记为 $\bigoplus_{i\in I} A_i$）.

每个 $m\in \sum_{i\in I} A_i$ 有形如

$$m=\sum_{i\in I}\alpha_i(a_i)$$

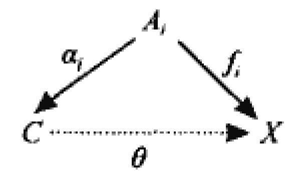
的唯一表达式，其中 $a_i\in A_i$. $\alpha_i(a_i)$ 是 $\prod A_i$ 中第 i 个坐标是 a_i 而其他坐标为 0 的 I 元组，且几乎一切 $a_i=0$；即只有有限个 a_i 非零.

注意如果指标集 I 是有限的，则 $\prod_{i\in I} A_i=\sum_{i\in I} A_i$. 另一方面，当 I 无限且有无限个 $A_i\neq 0$ 时，直和是直积的真子模（此外，在这种情形下，它们几乎永不同构）.

我们现在推广余积和积的概念到对象族.

451

定义 设 C 是范畴，$\{A_i : i\in I\}$ 是 C 中由集合 I 加标的对象族. **余积**是指由一个对象 $C=\bigsqcup_{i\in I} A_i$ 和一族内射态射 $\{\alpha_i$：对一切 $i\in I, A_i\to C\}$ 组成的有序对 $(C, \{\alpha_i : A_i\to C\})$，且满足下面的性质. 对每个配置有态射 $f : A_i\to X$ 的对象 X，存在唯一的态射 $\theta : C\to X$ 使得对每个 i 下图交换：



如果余积存在，用 $\bigsqcup_{i\in I} A_i$ 表示余积，且不计等价的话它是唯一的.

我们略述集合 $\{A_i : i\in I\}$ 的不相交并的存在性. 首先，构成集合 $B=\left(\bigcup_{i\in I} A_i\right)\times I$，然后定义

$$A_i'=\{(a_i, i)\in B : a_i\in A_i\}$$

于是不相交并为 $\bigsqcup_{i\in I} A_i=\bigcup_{i\in I} A'_i$（当然，两个集合的不相交并是这一构造的特殊情形）. 读者可以证明 $\bigsqcup_i A_i$ 连同由 $\alpha_i : a_i\mapsto (a_i, i)\in \bigsqcup_i A_i$ 给出的函数 $\alpha_i : A_i\to \bigsqcup_i A_i$ 组成集合范畴中的余积；即我们已经描述了泛映射问题的一个解.

命题 7.30 如果 $\{A_i : i\in I\}$ 是 R-模的族，则直和 $\sum_{i\in I} A_i$ 是它们在 ${}_R\mathbf{Mod}$ 范畴中的余积.

证明 命题的陈述不完全，余积需要内射态射 α_i. 记 $\sum_{i\in I} A_i$ 为 C，定义 $\alpha_i : A_i\to C$ 为 $a_i\mapsto \alpha_i(a)$ 如下：如果 $a_i\in A_i$，则 $\alpha_i(a_i)\in C$ 是第 i 个坐标是 a_i 而其他坐标都是零的 I 元组.

现在设 X 是模，且对每个 $i\in I$，设 $f_i : A_i\to X$ 是同态. 定义 $\theta : C\to X$ 为 $\theta : (a_i)\mapsto \sum_i f_i(a_i)$（注意，因为只有有限个 a_i 非零，所以这个和是有意义的）. 首先，图交换：如果 $a_i\in A_i$，则 $\theta\alpha_i(a_i)=f_i(a_i)$. 最后，$\theta$ 是唯一的. 如果 $\psi : C\to X$ 使得图交换，则 $\psi((a_i))=f_i(a_i)$. 因 ψ 是同态，有

$$\begin{aligned}\psi((a_i)) &= \psi\Big(\sum_i \alpha_i(a_i)\Big)\\ &= \sum_i \psi\alpha_i(a_i)=\sum_i f_i(a_i).\end{aligned}$$

所以 $\psi=\theta$. ■

我们给出 θ 的明确的公式．如果 $f_i: A_i \to X$ 是给定的同态，则 $\theta: \sum_{i\in I} A_i \to X$ 由

$$\theta:(a_i) \mapsto \sum_{i\in I} f_i(a_i)$$

452

给出［当然几乎一切 $a_i = 0$，从而在和 $\sum_{i\in I} f_i(a_i)$ 中只有有限个非零项］．

下面是对偶概念．

定义 设 $\mathcal{C}$ 是范畴，并设 $\{A_i : i \in I\}$ 是用集合 I 加标的 $\mathcal{C}$ 中对象的族．一个积是指由一个对象 C 和一个投射态射的族 $\{p_i : C \to A_i$ 对一切 $i \in I\}$ 组成的有序对 $(C, \{p_i : C \to A_i\})$，满足下列条件：对每个配置有态射 $f_i : X \to A_i$ 的对象 X，存在唯一的态射 $\theta: X \to C$ 使得对每个 i 下图交换：

$$\begin{array}{ccc} & A_i & \\ {}^{p_i}\nearrow & & \nwarrow^{f_i} \\ C & \xleftarrow[\theta]{} & X \end{array}$$

如果积存在，用 $\prod_{i\in I} A_i$ 表示积，且不计等价的话，它是唯一的．

我们让读者证明笛卡儿积是集合范畴中的积．

命题 7.31 如果 $\{A_i : i \in I\}$ 是 R-模的族，则直积 $C = \prod_{i\in I} A_i$ 是它们在 $_R\mathbf{Mod}$ 范畴中的积．

证明 命题的陈述不完全，因为积需要投射．对每个 $j \in I$，定义 $p_j : C \to A_j$ 为 $p_j : (a_i) \mapsto a_j \in A_j$．现在设 X 是模，且对每个 $i \in I$，设 $f_i : X \to A_i$ 是同态．定义 $\theta: X \to C$ 为 $\theta: x \mapsto (f_i(x))$．首先，图交换：如果 $x \in X$，则 $p_i\theta(x) = f_i(x)$．最后，θ 是唯一的．如果 $\psi: X \to C$ 使得图交换，则对一切 i，$p_i\psi(x) = f_i(x)$，即对每个 i，$\psi(x)$ 的第 i 个坐标是 $f_i(x)$，它也是 $\theta(x)$ 的第 i 个坐标．所以对一切 $x \in X$，$\psi(x) = \theta(x)$，从而 $\psi = \theta$． ■

范畴的观点使得下面两个证明十分简单．

定理 7.32 设 R 是交换环．对每个 R-模 A 和每个 R-模的族 $\{B_i : i \in I\}$，经 R-同构

$$\varphi: f \mapsto (p_i f),$$

有

$$\mathrm{Hom}_R(A, \prod_{i\in I} B_i) \cong \prod_{i\in I} \mathrm{Hom}_R(A, B_i),$$

其中 p_i 是积 $\prod_{i\in I} B_i$ 的投射．

证明 易知 φ 是可加的．为证明 φ 是 R-映射，注意对每个 i 和每个 $r \in R$，有 $p_i rf = rp_i f$；所以

453

$$\varphi: rf \mapsto (p_i rf) = (rp_i f) = r(p_i f) = r\varphi(f).$$

我们证明 φ 是满射．如果 $(f_i) \in \prod \mathrm{Hom}_R(A, B_i)$，则对每个 i，$f_i : A \to B_i$．

$$\begin{array}{ccc} & B_i & \\ {}^{p_i}\nearrow & & \nwarrow^{f_i} \\ \prod B_i & \xleftarrow[\theta]{} & A \end{array}$$

根据命题 7.31，$\prod B_i$ 是 $_R\mathbf{Mod}$ 范畴中的积，因此有唯一的 R-映射 $\theta: A \to \prod B_i$ 使得对每个 i，$p_i\theta = f_i$．于是 $(f_i) = \varphi(\theta)$，从而 φ 是满射．

为证明 φ 是单射，假设 $f \in \ker\varphi$，即 $0 = \varphi(f) = (p_i f)$. 于是对每个 $i, p_i f = 0$. 因此下面包含 f 的图交换：

$$\begin{array}{ccc} & B_i & \\ {}^{p_i}\nearrow & & \nwarrow^{0} \\ \prod B_i & \xleftarrow[f]{} & A \end{array}$$

但零同态也使得图交换，因此箭头 $A \to \prod B_i$ 的唯一性给出 $f = 0$. ■

定理 7.33 对每个 R-模 B 和每个 R-模的族 $\{A_i : i \in I\}$，经 R-同构

$$f \mapsto (f\alpha_i),$$

有

$$\mathrm{Hom}_R\Big(\sum_{i\in I} A_i, B\Big) \cong \prod_{i\in I} \mathrm{Hom}_R(A_i, B),$$

其中 α_i 是和 $\sum_{i\in I} A_i$ 的内射.

证明 这个证明与定理 7.32 的证明类似，留给读者. ■

有 $\mathrm{Hom}_R\big(A, \sum_i B_i\big) \ncong \sum_i \mathrm{Hom}_R(A, B_i)$ 和 $\mathrm{Hom}_R\big(\prod_i A_i, B\big) \ncong \prod_i \mathrm{Hom}_R(A_i, B)$ 的例子.

系 7.34 如果 A, A', B 和 B' 都是 R-模，则有同构

$$\mathrm{Hom}_R(A, B \sqcup B') \cong \mathrm{Hom}_R(A, B) \sqcup \mathrm{Hom}_R(A, B')$$

和

$$\mathrm{Hom}_R(A \sqcup A', B) \cong \mathrm{Hom}_R(A, B) \sqcup \mathrm{Hom}_R(A', B).$$

证明 当指标集有限时，模的直和与直积相等. ■ [454]

例 7.35 (i) 在例 7.6 中，我们定义域 k 上的向量空间 V 的对偶空间 V^* 为它的一切线性泛函的向量空间：

$$V^* = \mathrm{Hom}_k(V, k).$$

如果 $\dim(V) = n < \infty$，则例 5.6 表明 $V = V_1 \oplus \cdots \oplus V_n$，其中每个 V_i 都是一维空间. 根据系 7.34，$V^* \cong \sum_i \mathrm{Hom}_k(V_i, k)$ 是 n 个一维空间的直和 [因为习题 7.5 给出 $\mathrm{Hom}_k(k, k) \cong k$]，由此，习题 7.26 给出 $\dim(V^*) = \dim(V) = n$. 于是一个有限维向量空间和它的对偶空间同构. 由此当 V 是有限维向量空间时，由 $(V^*)^*$ 定义的二重对偶 V^{**} 和 V 同构.

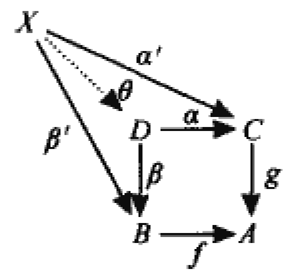
(ii) 有对偶空间的变种. 在泛函分析中，会遇到拓扑实向量空间，只要其上连续线性泛函有意义. 由一切连续线性泛函组成拓扑对偶 V^*，了解一个空间 V 是否自反是重要的，即对于这些空间是否有类似有限维空间的同构 $V \to V^{**}$ 这样的同态. 例如希尔伯特空间的自反性就是它的重要性质之一. ■

我们现在提出两种常用的对偶结构.

定义 在范畴 $\mathcal{C}$ 中给定两个态射 $f : B \to A$ 和 $g : C \to A$，一个解是指有序三元组 (D, α, β) 使得下图交换：

$$\begin{array}{ccc} D & \xrightarrow{\alpha} & C \\ {\scriptstyle\beta}\downarrow & & \downarrow{\scriptstyle g} \\ B & \xrightarrow[f]{} & A \end{array}$$

一个拉回（或纤维积）是指下列意义下的“最好”解 (D, α, β)：对每个解 (X, α', β')，存在唯一的态射 $\theta : X \to D$ 使得下图交换：



[455] 拉回存在时，如不计等价是唯一的，其证明与证明余积的唯一性是同一类型的．

命题 7.36　在 $_R\mathbf{Mod}$ 范畴中任两个映射 $f: B \to A$ 和 $g: C \to A$ 的拉回存在．

证明　定义

$$D = \{(b,c) \in B \sqcup C : f(b) = g(c)\},$$

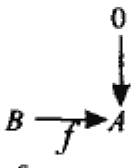
定义 $\alpha: D \to C$ 是投射 $(b,c) \mapsto c$ 的限制，定义 $\beta: D \to B$ 是投射 $(b,c) \mapsto b$ 的限制．易知 (D,α,β) 是一个解．

如果 (X,α',β) 是另一个解，定义映射 $\theta: X \to D$ 为 $\theta: x \mapsto (\beta'(x),\alpha'(x))$. 因为 X 是一个解，有 $f\beta'(x) = g\alpha'(x)$，所以 θ 的值在 D 中．我们留给读者证明图交换和 θ 唯一．■

例 7.37　(i) B 和 C 是集合 A 的子集可以重述为存在包含映射 $i: B \to A$ 和 $j: C \to A$. 读者可以证明集合范畴中拉回 D 存在，且有 $D = B \cap C$，并从中得到乐趣．

(ii) 在群范畴中存在拉回：它们是直积的某种子群，和命题 7.36 的证明中构造的一样．

(iii) 如果 $f: B \to A$ 是同态，则 $\ker f$ 是下图的拉回：



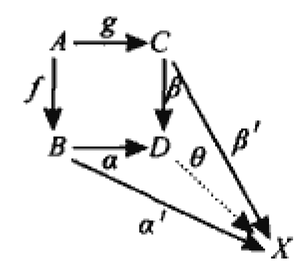
这个拉回是 $\{(b,0) \in B \sqcup \{0\} : fb = 0\} \cong \ker f$.　■

下面是对偶结构．

定义　在范畴$\mathcal{C}$中给定两个态射 $f: A \to B$ 和 $g: A \to C$，一个解是指有序三元组 (D,α,β) 使得下图交换：

$$\begin{array}{ccc} A & \xrightarrow{g} & C \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle \beta} \\ B & \xrightarrow{\alpha} & D \end{array}$$

[456] 一个**推出**（或纤维和）是指在下列意义下"最好"的解 (D,α,β)：对每个解 (X,α',β')，存在唯一的态射 $\theta: D \to X$ 使得下图交换：



又如果推出存在，则不计等价是唯一的．

命题 7.38　在 $_R\mathbf{Mod}$ 范畴中任两个映射 $f: A \to B$ 和 $g: A \to C$ 的推出存在．

证明　易知

$$S = \{(f(a), -g(a)) \in B \sqcup C : a \in A\}$$

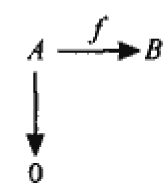
是 $B \sqcup C$ 的子模．定义 $D=(B \sqcup C)/S$，定义 $\alpha: B \to D$ 为 $b \mapsto (b,0)+S$，定义 $\beta: C \to D$ 为 $c \mapsto (0,c)+S$. 易知 (D,α,β) 是解．

给定另一个解 (X,α',β')，定义映射 $\theta: D \to X$ 为 $\theta:(b,c)+S \mapsto \alpha'(b)+\beta'(c)$. 我们还是让读者来证明图的交换性和 θ 的唯一性． ■

群范畴中的推出十分有趣．例如，两个单同态的推出叫做具有共合的自由积．

例 7.39 （ⅰ）如果 B 和 C 都是集合 A 的子集，则存在包含映射 $i: B \cap C \to B$ 和 $j: B \cap C \to C$. 读者可以证明集合范畴中推出 D 存在，且 D 是并 $B \cup C$，并从中得到乐趣．

（ⅱ）如果 $f: A \to B$ 是同态，则 $\operatorname{coker} f$ 是下图的推出：



毕竟这里的推出是商 $(\{0\} \sqcup B)/S$，其中 $S=\{(0,f(a))\}$，所以 $(\{0\} \sqcup B)/S \cong B/\operatorname{im} f=\operatorname{coker} f$. ■ [457]

习题

7.20 （ⅰ）证明在每个范畴 $\mathcal{C}$ 中，每个对象 $A \in \mathcal{C}$ 都有唯一的单位态射．

（ⅱ）如果 f 是范畴中的等价，证明它的逆唯一．

7.21 （ⅰ）设 X 是偏序集，并设 $a,b \in X$. 证明在 $\mathbf{PO}(X)$ 范畴中［它的定义在例7.25（ⅴ）中］，余积 $a \sqcup b$ 是 a 和 b 的最小上界，积 $a \sqcap b$ 是最大下界．

（ⅱ）设 Y 是集合，并令 $\mathcal{P}(Y)$ 表示它的幂集；即 Y 的一切子集的族．现在把 $\mathcal{P}(Y)$ 看作包含关系下的偏序集．如果 A 和 B 都是 Y 的子集，证明在 $\mathbf{PO}(\mathcal{P}(Y))$ 范畴中，余积 $A \sqcup B=A \cup B$，积 $A \sqcap B=A \cap B$.

（ⅲ）举出一个范畴的例子，其中有两个对象它们的余积不存在．

提示：见习题 6.43.

7.22 证明群范畴不是预加性范畴．

提示：如果 G 不是阿贝尔群，且 $f,g: G \to G$ 是同态，证明函数 $x \mapsto f(x)g(x)$ 可能不是同态．

7.23 如果 A 和 B 都是群（不必是阿贝尔群）．证明在群范畴中，$A \sqcap B=A \times B$（直积）．

7.24 如果 G 是有限阿贝尔群，证明 $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Q},G)=0$.

7.25 设 $\{M_i: i \in I\}$ 是模的族，且对每个 i 设 N_i 是 M_i 的子模．证明

$$\left(\sum_i M_i\right)/\left(\sum_i N_i\right) \cong \sum_i (M_i/N_i).$$

7.26 （ⅰ）设 $v_1,\cdots,v_n$ 是域 k 上向量空间 V 的基，从而每个 $v \in V$ 有唯一的表达式

$$v=a_1v_1+\cdots+a_nv_n,$$

其中对 $i=1,\cdots,n$ 有 $a_i \in k$. 证明对每个 i，由 $v_i^*: v \mapsto a_i$ 定义的函数 $v_i^*: V \to k$ 在对偶空间 V^* 中．

（ⅱ）证明 $v_1^*,\cdots,v_n^*$ 是 V^* 中的线性无关表．

（ⅲ）用例7.35（ⅰ）推出 $v_1^*,\cdots,v_n^*$ 是 V^* 的一个基（这组基叫做 $v_1,\cdots,v_n$ 的**对偶基**）．

（ⅳ）如果 $f: V \to V$ 是线性变换，设 A 是 f 关于 V 的基 $v_1,\cdots,v_n$ 的矩阵，即 A 的第 i 列由 $f(v_i)$ 在给定基 $v_1,\cdots,v_n$ 下的坐标组成．证明诱导映射 $f^*: V^* \to V^*$ 关于对偶基的矩阵是 A'，它是 A 的转置．

7.27 给定映射 $\sigma: \prod B_i \to \prod C_j$，求映射 $\tilde{\sigma}$ 使得下图交换：

$$\begin{array}{ccc} \operatorname{Hom}(A,\prod B_i) & \xrightarrow{\sigma} & \operatorname{Hom}(A,\prod C_j) \\ \downarrow \tau & & \downarrow \tau' \\ \prod \operatorname{Hom}(A,B_i) & \xrightarrow{\tilde{\sigma}} & \prod \operatorname{Hom}(A,C_j) \end{array}$$

[458]

其中 τ 和 τ' 是定理 7.32 的同构．

提示：如果 $f\in \mathrm{Hom}(A,\prod B_i)$，定义 $\tilde{\sigma}:(f_i)\mapsto(p_j\sigma f)$，即 $\tilde{\sigma}((f_i))$ 的第 j 个坐标是 $\sigma(f)\in\prod C_j$ 的第 j 个坐标．

7.28 (i) 给定 ${}_R\mathbf{Mod}$ 范畴中的一个推出图

$$\begin{array}{ccc} A & \xrightarrow{g} & C \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle \beta} \\ B & \xrightarrow[\alpha]{} & D \end{array}$$

证明 g 是单射蕴涵 α 是单射，g 是满射蕴涵 α 是满射．由此，平行的箭头有相同的性质．

(ii) 在${}_R\mathbf{Mod}$ 范畴中给定拉回图

$$\begin{array}{ccc} D & \xrightarrow{\alpha} & C \\ {\scriptstyle \beta}\downarrow & & \downarrow{\scriptstyle g} \\ B & \xrightarrow[f]{} & A \end{array}$$

证明 f 是单射蕴涵 α 是单射，f 是满射蕴涵 α 是满射．由此，平行的箭头有相同的性质．

7.29 **定义**：范畴$\mathcal{C}$中的一个对象 A 叫做**初对象**，如果对 $\mathcal{C}$中的每个对象 C，存在唯一的态射 $A\to C$．范畴 $\mathcal{C}$中的一个对象 Ω 叫做**终对象**，如果对$\mathcal{C}$中的每个对象 C，存在唯一的态射 $C\to\Omega$．

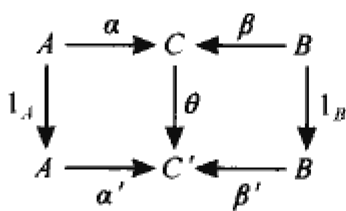
(i) 在初对象和终对象存在的情况下，证明它们的唯一性．举出一个没有初对象的范畴的例子．举出一个没有终对象的范畴的例子．

(ii) 如果 Ω 是范畴$\mathcal{C}$中的一个终对象，证明对任一 $G\in\mathrm{obj}(\mathcal{C})$，投射 $\lambda: G\sqcap\Omega\to G$ 和 $\rho:\Omega\sqcap G\to G$ 等价．

(iii) 设 A 和 B 都是范畴 $\mathcal{C}$ 中的对象．定义一个新范畴 $\mathcal{C}'$，它的对象是图

$$A\xrightarrow{\alpha}C\xleftarrow{\beta}B,$$

其中 C 是$\mathcal{C}$中的对象，α 和 β 是$\mathcal{C}$中的态射．定义 $\mathcal{C}'$ 中的态射为使得下图交换的$\mathcal{C}$中的态射 θ：



459

复合有一个明显的候选者．证明$\mathcal{C}'$是范畴．

(iv) 证明$\mathcal{C}'$中的一个初对象是$\mathcal{C}$中的一个余积．

(v) 给出一个类似的结构，证明积是一个适当范畴中的终对象．

7.30 范畴$\mathcal{C}$中的**零对象**是指既是初对象又是终对象的对象 Z.

(i) 证明在 ${}_R\mathbf{Mod}$ 范畴中，$\{0\}$ 是零对象．

(ii) 证明在集合范畴中，$\varnothing$是初对象．

(iii) 证明在集合范畴中，任一单点集都是终对象．

(iv) 证明在集合范畴中，不存在零对象．

7.31 (i) 假定余积存在，证明结合性：

$$A\sqcup(B\sqcup C)\cong(A\sqcup B)\sqcup C.$$

(ii) 假定积存在，证明结合性：

$$A\sqcap(B\sqcap C)\cong(A\sqcap B)\sqcap C.$$

7.32 设 C_1,C_2,D_1,D_2 都是范畴$\mathcal{C}$中的对象．

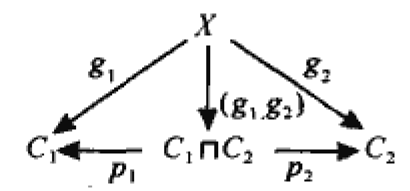
(i) 如果对 $i=1,2$ 存在态射 $f_i:C_i\to D_i$，且 $C_1\sqcap C_2$ 和 $D_1\sqcap D_2$ 都存在，证明存在唯一的态射 $f_1\sqcap f_2$

使得下图交换：

$$\begin{array}{ccc} C_1 \sqcap C_2 & \xrightarrow{f_1 \sqcap f_2} & D_1 \sqcap D_2 \\ p_i \downarrow & & \downarrow q_i \\ C_i & \xrightarrow[f_i]{} & D_i \end{array}$$

其中 p_i 和 q_i 都是投射．

（ⅱ）如果存在态射 $g_i : X \to C_i$，其中 X 是$\mathcal{C}$中 的一个对象，且 $i=1,2$，证明存在唯一的态射 (g_1, g_2) 使得下图交换：



其中 p_i 是投射．

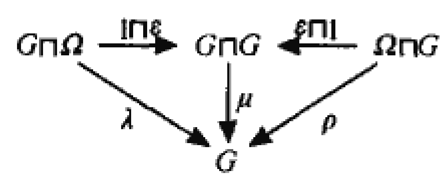
注：在集合范畴中，$(g_i, g_2) = (g_1 \sqcap g_2)\Delta_X$，其中 $\Delta_X : X \to X \times X$ 是对角线映射 $x \mapsto (x, x)$.

7.33　设$\mathcal{C}$是具有有限积和一个终对象 Ω 的范畴．$\mathcal{C}$中的一个群对象是指一个四元组 $(G, \mu, \eta, \varepsilon)$，其中 G 是$\mathcal{C}$中的一个对象，$\mu : G \sqcap G \to G, \eta : G \to G, \varepsilon : \Omega \to G$ 都是态射，从而下面的一些图交换：

结合性：

$$\begin{array}{ccc} G \sqcap G \sqcap G & \xrightarrow{1 \sqcap \mu} & G \sqcap G \\ \mu \sqcap 1 \downarrow & & \downarrow \mu \\ G \sqcap G & \xrightarrow[\mu]{} & G \end{array}$$

恒等：



其中 λ 和 ρ 都是习题7.29（ⅱ）中的等价．

逆：

$$\begin{array}{ccccc} G & \xrightarrow{(1,\eta)} & G \sqcap G & \xleftarrow{(\eta,1)} & G \\ \omega \downarrow & & \downarrow \mu & & \downarrow \omega \\ \Omega & \xrightarrow[\varepsilon]{} & G & \xleftarrow[\varepsilon]{} & \Omega \end{array}$$

其中 $\omega : G \to \Omega$ 是到终对象的唯一态射．

（ⅰ）证明集合范畴中的群对象是群．

（ⅱ）证明群范畴中的群对象是阿贝尔群．

提示：用习题 2.73.

7.3　函子

函子[⊖]是范畴的同态．

定义　回忆 $\text{obj}(\mathcal{C})$ 表示范畴$\mathcal{C}$中一切对象的类．如果$\mathcal{C}$和$\mathcal{D}$都是范畴，则函子 $T : \mathcal{C} \to \mathcal{D}$ 是指满足

⊖　术语 functor（函子）是哲学家卡纳普（R. Carnap）创造的，麦克莱恩认为它是这里的合适术语．

460

下列条件的函数：

（ⅰ）如果 $A \in \mathrm{obj}(\mathcal{C})$，则 $T(A) \in \mathrm{obj}(\mathcal{D})$；

（ⅱ）如果在$\mathcal{C}$中 $f: A \to A'$，则在$\mathcal{D}$中 $T(f): T(A) \to T(A')$；

（ⅲ）如果在$\mathcal{C}$中 $A \xrightarrow{f} A' \xrightarrow{g} A''$，则在$\mathcal{D}$中 $T(A) \xrightarrow{T(f)} T(A') \xrightarrow{T(g)} T(A'')$，且

$$T(gf) = T(g)T(f);$$

（ⅳ）对每个 $A \in \mathrm{obj}(\mathcal{C})$，

$$T(1_A) = 1_{T(A)}.$$

例 7.40 （ⅰ）如果$\mathcal{C}$是范畴，则**单位函子** $1_{\mathcal{C}}: \mathcal{C} \to \mathcal{C}$ 定义为

$$对一切对象\ A, 1_{\mathcal{C}}(A) = A,$$

以及

[461]

$$对一切态射\ f, 1_{\mathcal{C}}(f) = f.$$

（ⅱ）如果 $\mathcal{C}$是范畴，$A \in \mathrm{obj}(\mathcal{C})$，则 **Hom 函子** $T_A: \mathcal{C} \to$ 集合范畴定义为

$$对一切\ B \in \mathrm{obj}(\mathcal{C}), T_A(B) = \mathrm{Hom}(A,B),$$

如果在 $\mathcal{C}$中 $f: B \to B'$，则 $T_A(f): \mathrm{Hom}(A,B) \to \mathrm{Hom}(A,B')$ 由

$$T_A(f): h \mapsto fh$$

给出．我们称 $T_A(f)$ 为**诱导映射**，并把它记为

$$T_A(f) = f_*: h \mapsto fh.$$

因为这个例子的重要性，我们将详细验证定义的各部分．首先，正是范畴的定义说 $\mathrm{Hom}(A,B)$ 是集合．注意复合 fh 有意义：

$$A \xrightarrow{h} B \xrightarrow{f} B' \quad (hf)$$

现在假设 $g: B' \to B''$．我们比较函数

$$(gf)_*, g_* f_*: \mathrm{Hom}(A,B) \to \mathrm{Hom}(A,B'').$$

如果 $h \in \mathrm{Hom}(A,B)$，即 $h: A \to B$，则

$$(gf)_*: h \mapsto (gf)h;$$

另一方面，正如所要的

$$g_* f_*: h \mapsto fh \mapsto g(fh).$$

最后，如果 f 是恒等映射 $1_B: B \to B$，则对一切 $h \in \mathrm{Hom}(A,B)$，

$$(1_B)_*: h \mapsto 1_B h = h,$$

从而 $(1_B)_* = 1_{\mathrm{Hom}(A,B)}$．

如果记 $\mathrm{Hom}(A,\ )$ 为 T_A，则定理 7.32 说 T_A 保持积：$T_A(\prod_i B_i) \cong \prod_i T_A(B_i)$．

（ⅲ）如果 R 是交换环且 A 是 R-模，则 Hom 函子 $T_A: {}_R\mathbf{Mod} \to$ 集合范畴有更多的结构．我们在命题 7.5 中已经看到 $\mathrm{Hom}_R(A,B)$ 是 R- 模，现在证明：如果 $f: B \to B'$，则由 $h \mapsto fh$ 给出的诱导映射 $f_*: \mathrm{Hom}_R(A,B) \to \mathrm{Hom}_R(A,B')$ 是 R- 映射．首先，f_* 是可加的：如果 $h, h' \in \mathrm{Hom}(A,B)$，则对一切 $a \in A$，

$$\begin{aligned} f_*(h+h') &= f(h+h'): a \mapsto f(ha+h'a) \\ &= fha + fh'a = (f_*(h) + f_*(h'))(a), \end{aligned}$$

[462]

因此 $f_*(h+h') = f_*(h) + f_*(h')$．其次，$f_*$ 保持标量．回忆如果 $r \in R$ 和 $h \in \mathrm{Hom}(A,B)$，则

$rh: a \mapsto h(ra)$. 于是,

$$f_*(rh): a \mapsto f(rh)(a) = fh(ra),$$

而

$$rf_*(h) = rfh: a \mapsto fh(ra).$$

所以, $f_*(rh) = (rf)_*(h)$.

特别地, 如果 R 是域, 则诸 Hom_R 是向量空间, 诱导映射是线性变换.

(iv) 设$\mathcal{C}$是范畴, 并设 $A \in \mathrm{obj}(\mathcal{C})$. 定义 $T: \mathcal{C} \to \mathcal{C}$为对每个$C \in \mathrm{obj}(\mathcal{C})$, $T(C) = A$, 且对$\mathcal{C}$中每个态射 f, $T(f) = 1_A$. 则 T 是一个函子, 叫做 A 处的**常数函子**.

(v) 如果$\mathcal{C}$ = 群范畴, 定义**底函子** U:群范畴 → 集合范畴如下: $U(G)$ 是群 G 的"底"集, $U(f)$ 是仅仅看作函数的同态 f. 严格地说, 一个群是一个有序对(G,μ), 其中 G 是它的(底)集, $\mu: G\times G \to G$ 是它的运算, 而 $U((G,\mu))=G$, 函子 U "忘记"运算而只记住集合.

有许多变种. 例如, 一个 R-模是有序三元组(M,α,σ), 其中 M 是一个集合, $\alpha: M\times M \to M$ 是加法, $\sigma: R\times M \to M$ 是标量乘法. 有 $U'(M,\alpha,\sigma) = (M,\alpha)$ 的底函子 $U': {}_R\mathbf{Mod} \to \mathbf{Ab}$, 还有 $U''(M,\alpha,\sigma) = M$ 的底函子 $U'': {}_R\mathbf{Mod} \to$ 集合范畴. ■

下面的结果是有用的, 即使它十分容易证明.

命题 7.41 如果 $T: \mathcal{C} \to \mathcal{D}$是函子, 且 $f: A \to B$ 是$\mathcal{C}$中的等价, 则 $T(f)$ 是$\mathcal{D}$中的等价.

证明 如果 g 是 f 的逆, 运用 T 到等式

$$gf = 1_A \text{ 和 } fg = 1_B. \quad ■$$

这个命题从根本上说明为什么给出范畴的定义是有用的: 函子认可只用对象、态射和图来下定义. 在 **Ab** 范畴中, 如果把同构看作既是单射又是满射的同态, 那么如何证明这个结果?

还有第二种类型的函子, 它反转箭头的方向.

定义 如果 $\mathcal{C}$和$\mathcal{D}$都是范畴, 则**反变函子** $T:\mathcal{C} \to \mathcal{D}$ 是指一个函数满足

(i) 如果 $C \in \mathrm{obj}(\mathcal{C})$, 则 $T(C) \in \mathrm{obj}(\mathcal{D})$;

(ii) 如果在 $\mathcal{C}$中 $f: C \to C'$, 则在$\mathcal{D}$中 $T(f): T(C') \to T(C)$;

463

(iii) 如果在$\mathcal{C}$中 $C \xrightarrow{f} C' \xrightarrow{g} C''$, 则在 $\mathcal{D}$中 $T(C'') \xrightarrow{T(g)} T(C') \xrightarrow{T(f)} T(C)$ 且

$$T(gf) = T(f)T(g);$$

(iv) 对每个 $A \in \mathrm{obj}(\mathcal{C})$,

$$T(1_A) = 1_{T(A)}.$$

为了和反变函子相区别, 称早先定义的函子为**共变函子**.

例 7.42 (i) 如果$\mathcal{C}$是范畴, $B \in \mathrm{obj}(\mathcal{C})$, 则定义**反变 Hom 函子** $T^B: \mathcal{C} \to$ 集合范畴如下: 对一切 $C \in \mathrm{obj}(\mathcal{C})$,

$$T^B(C) = \mathrm{Hom}(C,B).$$

如果在$\mathcal{C}$中 $f: C \to C'$, 则 $T^B(f): \mathrm{Hom}(C',B) \to \mathrm{Hom}(C,B)$ 由

$$T^B(f): h \mapsto hf$$

给出. 我们称 $T^B(f)$ 为**诱导映射**, 并记为

$$T^B(f) = f^*: h \mapsto hf.$$

因为该例子的重要性, 我们验证表明 T^B 是(反变)函子的公理. 注意复合 hf 有意义:

$$C \xrightarrow{f} C' \xrightarrow{h} B \quad (hf: C \to B)$$

给定同态

$$C \xrightarrow{f} C' \xrightarrow{g} C'',$$

我们比较函数

$$(gf)^*, f^*g^*: \mathrm{Hom}(C'', B) \to \mathrm{Hom}(C, B).$$

如果 $h \in \mathrm{Hom}(C'', B)$（即如果 $h: C'' \to B$），则

$$(gf)^*: h \mapsto h(gf);$$

另一方面，正如所要的

$$f^*g^*: h \mapsto hg \mapsto (hg)f.$$

最后，如果 f 是恒等映射 $1_C: C \to C$，则对一切 $h \in \mathrm{Hom}(C, B)$，

464

$$(1_C)^*: h \mapsto h1_C = h.$$

因此 $(1_C)^* = 1_{\mathrm{Hom}(C,B)}$.

如果把 $\mathrm{Hom}(\ ,B)$ 记为 T^B，则定理 7.33 说反变函子 T^B 把和转变为积：$T^B(\sum_i A_i) \cong \prod_i T^B(A_i)$.

（ii）如果 R 是交换环，C 是 R-模，则反变 Hom 函子${}_R\mathbf{Mod} \to$ 集合范畴有更多结构．我们证明：如果 $f: C \to C'$ 是 R-映射，则由 $h \mapsto hf$ 给出的诱导映射 $f^*: \mathrm{Hom}_R(C', B) \to \mathrm{Hom}_R(C, B)$ 是 R-模之间的 R-映射．首先，f^* 是可加的：如果 $g, h \in \mathrm{Hom}(C', B)$，则对一切 $c' \in C'$，

$$\begin{aligned} f^*(g+h) = (g+h)f &: c' \mapsto (g+h)f(c') \\ &= gfc' + hfc' = (f^*(g) + f^*(h))(c'), \end{aligned}$$

因此 $f^*(g+h) = f^*(h) + f^*(g)$．其次，$f^*$ 保持标量．回忆如果 $r \in R$ 和 $h \in \mathrm{Hom}(A, B)$，则 $rh: a \mapsto h(ra)$．由此，

$$f^*(rh): c' \mapsto (rh)f(c') = h(rf(c')),$$

而

$$rf^*(h) = r(hf): c' \mapsto hf(rc').$$

因为 $rf(c') = f(rc')$，所以两者相同，从而 $f^*(rh) = rf^*(h)$.

特别地，如果 R 是域，则诸 Hom_R 是向量空间且诱导映射是线性变换．一个特殊情形是**对偶空间函子** $\mathrm{Hom}_k(\ ,k)$，其中 k 是域. ■

易知，和命题 7.41 一样，每个反变函子保持等价，即如果 $T: \mathcal{C} \to \mathcal{D}$ 是反变函子，且如果 $f: C \to C'$ 是$\mathcal{C}$中的等价，则 $T(f)$ 是$\mathcal{D}$中的等价．

定义 假定$\mathcal{C}$和$\mathcal{D}$都是预加性范畴，则共变或反变函子 $T: \mathcal{C} \to \mathcal{D}$ 称为**加性函子**，如果对每对态射 $f, g: A \to B$ 有

$$T(f+g) = T(f) + T(g).$$

易知共变或反变 Hom 函子${}_R\mathbf{Mod} \to \mathbf{Ab}$ 是加性函子．

每个共变函子 $T: \mathcal{C} \to \mathcal{D}$对每个 A 和 B 给出函数

$$T_{AB}: \mathrm{Hom}(A, B) \to \mathrm{Hom}(TA, TB),$$

它由 $h \mapsto T(h)$ 定义．如果 T 是两个预加性范畴之间的加性函子，则每个 T_{AB} 都是阿贝尔群的同态.

类似的陈述对反变函子也成立.

465

下面是系 7.34 的适度推广.

命题 7.43 如果 $T: {}_R\mathbf{Mod} \to \mathbf{Ab}$ 是共变或反变加性函子，则 T 保持有限直和：

$$T(A_1 \oplus \cdots \oplus A_n) \cong T(A_1) \oplus \cdots \oplus T(A_n).$$

证明 根据归纳法，只需证明 $T(A \oplus B) \cong T(A) \oplus T(B)$. 命题7.15(ⅲ)用映射 $p: M \to A$，$q: M \to B$，$i: A \to M$ 和 $j: B \to M$ 满足

$$pi = 1_A, qj = 1_B, pj = 0, qi = 0 \text{ 和 } ip + jq = 1_M$$

刻画了 $M = A \oplus B$. 因 T 是加性函子，习题 7.34 给出 $T(0) = 0$，因此 T 保持这些等式. ■

刚才我们已经看到加性函子 $T: {}_R\mathbf{Mod} \to \mathbf{Ab}$ 保持两个模的直和：

$$T(A \oplus C) = T(A) \oplus T(C).$$

如果把这样的直和看作分裂短正合列，则可以作这样的陈述：如果

$$0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$$

是分裂短正合列，则

$$0 \to T(A) \xrightarrow{T(i)} T(B) \xrightarrow{T(p)} T(C) \to 0$$

也是分裂短正合列. 由此导致更一般的问题：如果

$$0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$$

是任一短正合列，未必分裂，那么

$$0 \to T(A) \xrightarrow{T(i)} T(B) \xrightarrow{T(p)} T(C) \to 0$$

也是正合列吗? 下面是对 Hom 函子的回答（定理陈述中没有印刷错误："$\to 0$"不必出现在序列的末端，我们在证明之后讨论这一点).

定理 7.44 如果

$$0 \to A \xrightarrow{i} B \xrightarrow{p} C$$

是 R-模的正合列，且 X 是一个 R-模，则存在正合列

$$0 \to \mathrm{Hom}_R(X,A) \xrightarrow{i_*} \mathrm{Hom}_R(X,B) \xrightarrow{p_*} \mathrm{Hom}_R(X,C).$$

466

证明 (ⅰ) $\ker i_* = \{0\}$：

如果 $f \in \ker i_*$，则 $f: X \to A$ 和 $i_*(f) = 0$；即

$$\text{对一切 } x \in X, if(x) = 0.$$

因 i 是单射，对一切 $x \in X, f(x) = 0$，因此 $f = 0$.

(ⅱ) $\mathrm{im}\, i_* \subseteq \ker p_*$：

如果 $g \in \mathrm{im}\, i_*$，则 $g: X \to B$ 和有某个 $f: X \to A$ 使得 $g = i_*(f) = if$. 但由于原始序列的正合性，也就是 $\mathrm{im}\, i = \ker p$ 蕴涵 $pi = 0$，所以 $p_*(g) = pg = pif = 0$.

(ⅲ) $\ker p_* \subseteq \mathrm{im}\, i_*$：

如果 $g \in \ker p_*$，则 $g: X \to B$ 和 $p_*(g) = pg = 0$. 因此对一切 $x \in X, pg(x) = 0$，从而 $g(x) \in \ker p = \mathrm{im}\, i$. 由此，存在某个 $a \in A$ 使得 $g(x) = i(a)$；因 i 是单射，这个元素 a 是唯一的. 因此如下给出的函数 $f: X \to A$：如果 $g(x) = i(a)$ 则 $f(x) = a$，是合理定义的. 容易验证 $f \in \mathrm{Hom}_R(X, A)$；即 f 是 R-同态. 因

$$g(x+x')=g(x)+g(x')=i(a)+i(a')=i(a+a'),$$

所以有

$$f(x+x')=a+a'=f(x)+f(x').$$

类似的论证表明对一切 $r\in R, f(rx)=rf(x)$. 但 $i_*(f)=if$ 且对一切 $x\in X, if(x)=i(a)=g(x)$；即 $i_*(f)=g$，从而 $g\in \mathrm{im}i_*$. ■

例 7.45 即使假定在原来的正合列中映射 $p: B\to C$ 是满射，经函子作用后的序列也未必以"$\to 0$"结尾，即 $p_*: \mathrm{Hom}_R(X,B)\to \mathrm{Hom}_R(X,C)$ 可能不是满射.

阿贝尔群$\mathbb{Q}/\mathbb{Z}$由一切陪集 $q+\mathbb{Z}$（其中 $q\in\mathbb{Q}$）组成，易知它的元素 $\frac{1}{2}+\mathbb{Z}$ 的阶为 2. 由此 $\mathrm{Hom}_\mathbb{Z}(\mathbb{I}_2,\mathbb{Q}/\mathbb{Z})\neq\{0\}$，因为它包含非零同态 $[1]\mapsto\frac{1}{2}+\mathbb{Z}$.

把函子 $\mathrm{Hom}_\mathbb{Z}(\mathbb{I}_2,\ )$ 作用到

$$0\to\mathbb{Z}\xrightarrow{i}\mathbb{Q}\xrightarrow{p}\mathbb{Q}/\mathbb{Z}\to 0$$

上，其中 i 是包含映射，p 是自然映射. 我们刚才已经看到

$$\mathrm{Hom}_\mathbb{Z}(\mathbb{I}_2,\mathbb{Q}/\mathbb{Z})\neq\{0\};$$

另一方面，因为$\mathbb{Q}$没有有限阶的（非零）元素，$\mathrm{Hom}_\mathbb{Z}(\mathbb{I}_2,\mathbb{Q})=\{0\}$. 所以诱导映射 $p_*: \mathrm{Hom}_\mathbb{Z}(\mathbb{I}_2,\mathbb{Q})\to \mathrm{Hom}_\mathbb{Z}(\mathbb{I}_2,\mathbb{Q}/\mathbb{Z})$ 不可能是满射. ■

467

定义 共变函子 $T: {}_R\mathbf{Mod}\to\mathbf{Ab}$ 称为**左正合的**，如果

$$0\to A\xrightarrow{i}B\xrightarrow{p}C$$

的正合性蕴涵

$$0\to T(A)\xrightarrow{T(i)}T(B)\xrightarrow{T(p)}T(C)$$

的正合性.

这样，定理 7.44 表明共变 Hom 函子 $\mathrm{Hom}_R(X,\ )$ 是左正合的. 在同调代数中研究了 $\mathrm{Hom}_R(X,\ )$ 的余核，它涉及叫做 $\mathrm{Ext}^1_R(X,\ )$ 的函子.

对反变 Hom 函子有一个类似的结果

定理 7.46 如果

$$A\xrightarrow{i}B\xrightarrow{p}C\to 0$$

是 R-模的正合列，且 Y 是一个 R-模，则存在正合列

$$0\to\mathrm{Hom}_R(C,Y)\xrightarrow{p^*}\mathrm{Hom}_R(B,Y)\xrightarrow{i^*}\mathrm{Hom}_R(A,Y).$$

证明 （i）$\ker p^*=\{0\}$：

如果 $h\in\ker p^*$，则 $h: C\to Y$ 和 $0=p^*(h)=hp$. 于是对一切 $b\in B, h(p(b))=0$，因此对一切 $c\in \mathrm{im}p, h(c)=0$. 因 p 是满射，$\mathrm{im}p=C$，从而 $h=0$.

（ii）$\mathrm{im}p^*\subseteq\ker i^*$：

如果 $g\in\mathrm{Hom}_R(C,Y)$，则因原始序列的正合性，也就是 $\mathrm{im}i=\ker p$ 蕴涵 $pi=0$，所以

$$i^*p^*(g)=(pi)^*(g)=0.$$

（iii）$\ker i^*\subseteq\mathrm{im}p^*$：

如果 $g \in \ker i^*$，则 $g: B \to Y$ 和 $i^*(g) = gi = 0$. 如果 $c \in C$，则因 p 是满射，有某个 $b \in B$ 使得 $c = p(b)$. 定义 $f: C \to Y$ 为：如果 $c = p(b)$，则 $f(c) = g(b)$. 注意 f 是合理定义的：如果 $p(b) = p(b')$，则 $b - b' \in \ker p = \operatorname{im} i$，从而有某个 $a \in A$ 使得 $b - b' = i(a)$. 由于 $gi = 0$，因此

$$g(b) - g(b') = g(b - b') = gi(a) = 0.$$

读者可以验证 f 是 R-映射. 最后，如果 $c = p(b)$，则 $g(b) = f(c) = f(p(b))$，因此

$$p^*(f) = fp = g,$$

所以 $g \in \operatorname{im} p^*$. ■

468

例 7.47 即使假定在原来的正合列中映射 $i: A \to B$ 是单射，经函子作用的序列也未必以"$\to 0$"结尾，即 $i^*: \operatorname{Hom}_R(B,Y) \to \operatorname{Hom}_R(A,Y)$ 可能不是满射.

我们断言 $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z}) = 0$. 假设 $f: \mathbb{Q} \to \mathbb{Z}$ 且有某个 $a/b \in \mathbb{Q}$ 使得 $f(a/b) \neq 0$. 如果 $f(a/b) = m$，则对一切 $n > 0$，

$$nf(a/nb) = f(na/nb) = f(a/b) = m.$$

于是 m 被每个正整数 n 整除，此与算术基本定理矛盾.

如果把函子 $\operatorname{Hom}_{\mathbb{Z}}(\ ,\mathbb{Z})$ 作用到短正合列

$$0 \to \mathbb{Z} \xrightarrow{i} \mathbb{Q} \xrightarrow{p} \mathbb{Q}/\mathbb{Z} \to 0$$

上，其中 i 是包含映射，p 是自然映射，则诱导映射

$$i^*: \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z}) \to \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z})$$

不可能是满射，这是因为 $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z}) = \{0\}$，而由于 $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z})$ 包含 $1_{\mathbb{Z}}$，因此 $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) \neq \{0\}$. ■

定义 反变函子 $T: {}_R\mathbf{Mod} \to \mathbf{Ab}$ 称为左正合的，如果

$$A \xrightarrow{i} B \xrightarrow{p} C \to 0$$

的正合性蕴涵

$$0 \to T(C) \xrightarrow{T(p)} T(B) \xrightarrow{T(i)} T(A)$$

的正合性.

由此，定理 7.46 证明反变 Hom 函子 $\operatorname{Hom}_R(\ ,Y)$ 是左正合函子.[⊖]

定理 7.46 有逆定理，对共变 Hom 函子的对偶陈述也成立.

命题 7.48 设 $i: B' \to B$ 和 $p: B \to B''$ 都是 R-映射，其中 R 是交换环. 如果对某个 R-模 M，

$$0 \to \operatorname{Hom}_R(B'', M) \xrightarrow{p^*} \operatorname{Hom}_R(B, M) \xrightarrow{i^*} \operatorname{Hom}_R(B', M)$$

是正合列，则

$$B' \xrightarrow{i} B \xrightarrow{p} B'' \to 0$$

也是正合列.

469

证明 (i) p 是满射.

设 $M = B''/\operatorname{im} p$，并设 $f: B'' \to B''/\operatorname{im} p$ 是自然映射，从而 $f \in \operatorname{Hom}(B'', M)$. 由于 $p^*(f) = fp = 0$，且 p^* 是单射，从而 $f = 0$. 所以 $B''/\operatorname{im} p = 0$，$p$ 是满射.

⊖ 这些函子叫做左正合的是因为被函子作用的序列在左端有 $0 \to$.

(ⅱ) $\mathrm{im}i \subseteq \ker p$.

因 $i^* p^* = 0$，有 $0 = (pi)^*$. 因此，如果 $M = B''$ 和 $g = 1_{B''}$，从而 $g \in \mathrm{Hom}(B'',M)$，则 $0 = (pi)^* g = gpi = pi$，所以 $\mathrm{im}i \subseteq \ker p$.

(ⅲ) $\ker p \subseteq \mathrm{im}i$.

现在选取 $M = B/\mathrm{im}i$，并设 $h: B \to M$ 是自然映射，从而 $h \in \mathrm{Hom}(B,M)$. 显然 $i^* h = hi = 0$，因此 Hom 序列的正合性给出一个元素 $h' \in \mathrm{Hom}_R(B'',M)$ 使得 $p^*(h') = h'p = h$. 根据（ⅱ），有 $\mathrm{im}i \subseteq \ker p$，因此，如果 $\mathrm{im}i \neq \ker p$，则存在元素 $b \in B$ 但 $b \notin \mathrm{im}i$ 且 $b \in \ker p$. 于是 $hb \neq 0$ 和 $pb = 0$，由此产生矛盾 $hb = h'pb = 0$. ■

定义 称一个共变函子 $T: {}_R\mathbf{Mod} \to \mathbf{Ab}$ 为**正合函子**，如果

$$0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$$

的正合性蕴涵

$$0 \to T(A) \xrightarrow{T(i)} T(B) \xrightarrow{T(p)} T(C) \to 0$$

的正合性. 类似定义正合反变函子.

下一节中我们将看到对于某些选定的模，Hom 函子是正合函子.

习题

7.34 如果 $T: {}_R\mathbf{Mod} \to \mathbf{Ab}$ 是一个共变或反变加性函子，证明 $T(0) = 0$，其中 0 表示零模或零态射.

7.35 举出一个不保持余积的共变函子的例子.
提示：用习题7.21(ⅲ).

7.36 设 $\mathcal{A} \xrightarrow{S} \mathcal{B} \xrightarrow{T} \mathcal{C}$ 是函子. 证明复合 $\mathcal{A} \xrightarrow{TS} \mathcal{C}$ 是这样的函子，当 S 和 T 是相同的共变函子或反变函子时，它是共变函子，当 S 和 T 一个是共变函子另一个是反变函子时，它是反变函子.

7.37 (ⅰ) 证明在交换环范畴上有如下定义的函子：关于对象定义为 $R \mapsto R[x]$，关于态射 $f: R \to S$ 定义为 $r \mapsto f(r)$（即如果用 $R[x]$ 的元素的形式，记号就是 $(r,0,0,\cdots) \mapsto (f(r),0,0,\cdots)$）.

(ⅱ) 证明在 **Dom**（一切整环的范畴）上有如下定义的函子，关于对象定义为 $R \mapsto \mathrm{Frac}(R)$，关于态射 $f: R \to S$ 定义为 $r/1 \mapsto f(r)/1$.

470 7.38 证明存在群范畴 $\to \mathbf{Ab}$ 的函子使得每个群 G 变到 G/G'，其中 G' 是 G 换位子群.

7.39 (ⅰ) 如果 X 是集合，k 是域，定义向量空间 k^X 为点态运算下一切函数 $X \to k$ 的集合. 证明存在函子 F：集合范畴 $\to {}_k\mathbf{Mod}$ 使得 $F(X) = k^X$.

(ⅱ) 如果 X 是集合，定义 $F(X)$ 为以 X 为基的自由群. 证明存在函子 F：集合范畴$\to$群范畴使得 $F: X \mapsto F(X)$.

7.4 自由模、投射和内射

和群一样，最简单的模是自由模，每个模都是自由模的商；即每个模都可以用生成元和关系来表现. 投射模是自由模的推广，从而也是十分有用的. 作为投射模的对偶，我们定义内射模，但是一直要到第 10 章讨论同调代数时才会赏识它的价值. 此时，在这里将看到我们相当熟悉的内射Z-模.

定义 R-模 F 称为**自由 R-模**，如果 F 同构于若干个 R 复制的直和，即存在指标集 I（可以无限）使得

$$F = \sum_{i \in I} R_i,$$

其中对一切 $i, R_i = \langle b_i \rangle \cong R$. 我们称 $B = \{b_i : i \in I\}$ 为 F 的基.

自由 Z-模是自由阿贝尔群，每个交换环 R 看作它自身上的模时，是自由 R-模.

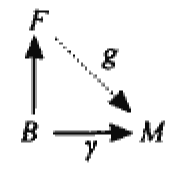
从直和的讨论中，我们知道每个 $m \in F$ 有唯一的形如

$$m = \sum_{i \in I} r_i b_i$$

的表达式，其中 $r_i \in R$ 且几乎一切 $r_i = 0$. 自由模的基和向量空间的基十分相像. 确实，容易看出域 k 上的向量空间 V 是一个自由 k-模，此时基的两个概念是一致的.

容易把定理 3.92 从有限维向量空间推广到任意自由模上（特别是推广到无限维向量空间上）.

命题 7.49 设 F 是由子集 B 生成的 R-模，则 F 是一个(同构于)以 B 为基的自由 R-模，当且仅当对任意 R-模 M 和任意函数 $\gamma: B \to M$，存在一个唯一的 R-映射 $g: F \to M$ 使得对一切 $b \in B, g(b) = \gamma(b)$.



471

证明 每个元素 $v \in F$ 有形如

$$v = \sum_{b \in B} r_b b$$

的唯一表达式，其中 $r_b \in R$ 且几乎一切 $r_b = 0$. 定义 $g: F \to M$ 为 $g(v) = \sum_{b \in B} r_b \gamma(b)$.

反之，如果定义 $A_b = Rb$，即以 $\{b\}$ 为基自由 R-模，则这个条件表明 F 是 $\{A_b : b \leftarrow B\}$ 的余积，更详细地说，定义内射 α_b，它把 $r_b b$ 映射到第 b 个坐标为 $r_b b$、其他坐标为 0 的"向量". 和任意余积一样，存在唯一的映射 $\theta: F \to M$ 使得 $\theta\alpha_b(b) = \gamma(b)$. 映射 θ 和 g 在基 B 的每个元素上一致，因此 $\theta = g$. 根据命题 7.30，$F \cong \sum_{b \in B} A_b = \sum_{b \in B} Rb$，所以 F 同构于以 B 为基的自由 R-模. ■

定义 基中元素的个数称为 F 的秩，记为 $\mathrm{rank}(F)$.

当然，秩类似于维数. 下一命题证明秩是合理定义的.

命题 7.50 (ⅰ) 如果 R 是非零交换环，则自由 R-模 F 的任意两个基有相同的基数，即元素个数相同.

(ⅱ) 如果 R 是非零交换环，则自由 R-模 F 和 F' 同构当且仅当 $\mathrm{rank}(F) = \mathrm{rank}(F')$.

证明 (ⅰ) 选取 R 中的极大理想 I(根据定理 6.46，极大理想存在). 如果 X 是自由 R-模 F 的一个基，则习题 7.6 表明陪集的集合 $\{v + IF : v \in X\}$ 是域 R/I 上的向量空间 F/IF 的一个基. 如果 Y 是 F 的另一个基，则同样的论证给出 $\{u + IF : u \in Y\}$ 是 F/IF 的基. 但向量空间的任意两个基大小相同(它是空间的维数)，从而根据定理 6.51，$|X| = |Y|$.

(ⅱ) 设 X 是 F 的基，X' 是 F' 的基，并设 $\gamma: X \to X'$ 是双射. 把 γ 和包含映射 $X' \to F'$ 复合起来，可以假定 $\gamma: X \to F'$. 根据命题 7.49，存在扩张 γ 的唯一 R-映射 $\varphi: F \to F'$. 同样，可以把 $\gamma^{-1}: X' \to X$ 看作函数 $X' \to F$，并存在扩张 γ^{-1} 的唯一映射 $\psi: F' \to F$. 最后，$\psi\varphi$ 和 1_F 都扩张 1_X，因此 $\psi\varphi = 1_F$. 同样，另一个复合是 $1_{F'}$，因此 $\varphi: F \to F'$ 是同构.（机敏的读者会注意到这个证明和泛映射问题解的唯一性的证明十分相像.）

反之，假定 $\varphi: F \to F'$ 是同构. 如果 $\{v_i : i \in I\}$ 是 F 的基，则易知 $\{\varphi(v_i) : i \in I\}$ 是 F' 基. 但根据(ⅰ)，自由模 F' 的任意两个基的大小相同，就是 $\mathrm{rank}(F')$. 因此 $\mathrm{rank}(F') = \mathrm{rank}(F)$. ■

[472] 下一命题使我们可以用自由模来描述任意模.

命题 7.51 每个 R-模 M 都是一个自由 R-模 F 的一个商. 此外, M 是有限生成的当且仅当 F 可以选取为有限生成的. ■

证明 设 R 是 R 的 $|M|$ 个复制的直和(从而 F 是自由模), 并设 $\{x_m : m \in M\}$ 是 F 的基. 根据命题 7.49, 存在 R-映射 $g : F \to M$ 使得对一切 $m \in M, g(x_m) = m$. 显然 g 是满射, 从而 $F/\ker g \cong M$.

如果 M 是有限生成的, 则 $M = \langle m_1, \cdots, m_n \rangle$. 如果选取 F 是以 $\{x_1, \cdots, x_n\}$ 为基的自由 R-模, 则满足 $g(x_i) = m_i$ 的映射 $g : F \to M$ 是满射, 这是因为

$$\operatorname{img} = \langle g(x_1), \cdots, g(x_n) \rangle = \langle m_1, \cdots, m_n \rangle = M.$$

逆命题显然成立, 因为有限生成模的象也是有限生成的. ■

上面的命题可以用来构造具有指定性质的模. 例如, 考虑 $\mathbb{Z}$-模 (即阿贝尔群). 群 $\mathbb{Q}/\mathbb{Z}$ 包含一个 2 阶元素 a, 它对一切 $n \geqslant 1$ 满足等式 $a = 2^n a_n$; 取 $a = \frac{1}{2} + \mathbb{Z}, a_n = 1/2^{n+1} + \mathbb{Z}$. 当然, 因为 $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Q}/\mathbb{Z})$ 包含自然映射, 所以 $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Q}/\mathbb{Z}) \neq \{0\}$. 存在阿贝尔群 G 使得 $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Q}, G) = \{0\}$ 且包含一个对一切 $n \geqslant 1$ 满足等式 $a = 2^n a_n$ 的 2 阶元素 a 吗? 设 F 是自由阿贝尔群, 有基

$$\{a, b_1, b_2, \cdots, b_n, \cdots\}$$

和关系

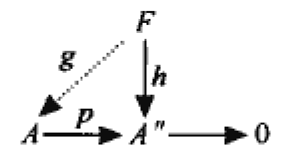
$$\{2a, a - 2^n b_n, n \geqslant 1\};$$

即设 K 是由 $\{2a, a - 2^n b_n, n \geqslant 1\}$ 生成的 F 的子群. 习题 7.48 要求读者验证 $G = F/K$ 满足所要的性质. 这个构造法是用生成元和关系来定义 R-模 (如同我们已经对群所做的那样) 的一个特殊情形.

定义 设 $\mathcal{X} = \{x_i : i \in I\}$ 是自由 R-模 F 的基, 并设 $\mathcal{R} = \left\{ \sum_i r_{ji} x_i : j \in J \right\}$ 是 F 的子集. 如果 K 是由 $\mathcal{R}$ 生成的 F 的子模, 则我们说模 $M = F/K$ 具有**生成元** $\mathcal{X}$ 和**关系** $\mathcal{R}$.[⊖] 我们也说有序对 $(\mathcal{X} \mid \mathcal{R})$ 是 M 的**表现**.

本节末将回到表现, 但现在为了得到一个关于自由模的不提及基的定理, 我们来关注基的关键性质, 即引理 7.49 (它对自由模成立, 对向量空间也成立).

定理 7.52 如果 R 是交换环, F 是自由 R-模, 则对每个满射 $p : A \to A''$ 和每个 $h : F \to A''$, 存在
[473] 同态 g 使得下图交换:



证明 设 $\{b_i : i \in I\}$ 是 F 的基. 因 p 是满射, 对一切 i 有 $a_i \in A$ 使得 $p(a_i) = h(b_i)$. 根据命题 7.49, 存在 R-映射 $g : F \to A$ 使得

$$\text{对一切 } i, g(b_i) = a_i.$$

现在 $pg(b_i) = p(a_i) = h(b_i)$, 从而 pg 和 h 在基 $\{b_i : i \in I\}$ 上一致, 由此在 $\langle \{b_i : i \in I\} \rangle = F$ 上 $pg = h$; 即 $pg = h$. ■

定义 称满足 $pg = h$ 的映射 $g : F \to A$ (定理 7.52 中的图) 为 h 的一个**提升**.

如果 C 是任意模, 不必是自由模, 则 h 的提升 g 如果存在的话未必唯一. 因 $pi = 0$, 其中 $i : \ker p$

⊖ 称一个模为自由的是因为它没有纠缠关系.

$\to A$ 是包含映射，则对任意 $f \in \mathrm{Hom}_R(C, \ker p)$，$g + if$ 也是 h 的提升．其实从正合列

$$0 \to \mathrm{Hom}(C, \ker p) \xrightarrow{i_*} \mathrm{Hom}(C, A) \xrightarrow{p_*} \mathrm{Hom}(C, A'')$$

来看是显然的．h 的任意两个提升由 $\ker p_* = \mathrm{im}\, i_* \subseteq \mathrm{Hom}(C, A)$ 中的一个映射来区分．

我们现在把自由模的这个（不提及基的）性质升级为一个定义．

定义 称模 P 为投射的，如果对任意的满射 p 和任意的映射 h，存在提升 g，即存在映射 g 使得下图交换：

$$\begin{array}{ccccc} & & P & & \\ & \overset{g}{\swarrow} & \downarrow h & & \\ A & \xrightarrow{p} & A'' & \to & 0 \end{array}$$

我们知道每个自由模都是投射的，那么每个投射 R-模都是自由模吗？我们将看到这个问题的答案依赖于环 R. 注意，如果投射 R-模正好是自由的，则可以不提及基来刻画自由模．

现在用一种自然的方式来看待投射模．我们知道 Hom 函子是左正合的，即对任意模 P 把 $\mathrm{Hom}_R(P, \ )$ 作用到正合列

$$0 \to A' \xrightarrow{i} A \xrightarrow{p} A''$$

上得正合列

$$0 \to \mathrm{Hom}_R(P, A') \xrightarrow{i_*} \mathrm{Hom}_R(P, A) \xrightarrow{p_*} \mathrm{Hom}_R(P, A'').$$

474

命题 7.53 模 P 是投射的当且仅当 $\mathrm{Hom}_R(P, \ )$ 是正合函子．

注 因 $\mathrm{Hom}_R(P, \ )$ 是左正合函子，这个命题的核心是当 p 是满射时，p_* 也是满射．

证明 如果 P 是投射模，则给定 $h: P \to A''$，存在提升 $g: P \to A$ 使得 $pg = h$. 于是，如果 $h \in \mathrm{Hom}_R(P, A'')$，则 $h = pg = p_*(g) \in \mathrm{im}\, p_*$，从而 p_* 是满射．因此 $\mathrm{Hom}_R(P, \ )$ 是正合函子．

关于逆命题，假定 $\mathrm{Hom}_R(P, \ )$ 是正合函子，从而 p_* 是满射：如果 $h \in \mathrm{Hom}_R(P, A'')$，则存在 $g \in \mathrm{Hom}_R(P, A)$ 使得 $h = p_*(g) = pg$. 这就是说，给定 p 和 h，存在提升 g 使得图交换；即 P 是投射模． ■

命题 7.54 模 P 是投射模当且仅当每个短正合列

$$0 \to A \xrightarrow{i} B \xrightarrow{p} P \to 0$$

分裂．

证明 如果 P 是投射模，则存在 $j: P \to B$ 使得下图交换；即 $pj = 1_P$．

$$\begin{array}{ccccc} & & P & & \\ & \overset{j}{\swarrow} & \downarrow 1_P & & \\ B & \xrightarrow{p} & P & \to & 0 \end{array}$$

现在系 7.17 给出结果．

反之，假定每个以 P 结束的短正合列分裂．考虑图

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow f & & \\ B & \xrightarrow{p} & C & \to & 0 \end{array}$$

其中 p 是满射．现在形成拉回

$$\begin{array}{ccccc} D & \underset{j}{\overset{\alpha}{\rightleftarrows}} & P & & \\ \beta\downarrow & & \downarrow f & & \\ B & \xrightarrow{p} & C & \longrightarrow & 0 \end{array}$$

根据习题 7.28，在拉回图中 p 的满射性给出 α 的满射性．根据假设，存在映射 $j: P \to D$ 使得 $\alpha j = 1_P$. 定义 $g: P \to B$ 为 $g = \beta j$．验证：

$$pg = p\beta j = f\alpha j = f1_P = f.$$

所以 P 是投射模． ■

475

我们重述该命题的一半从而不提及正合这个词．

系 7.55 *设 A 是模 B 的子模．如果 B/A 是投射的，则存在 B 的子模 C 使得 $C \cong B/A$ 和 $B = A \oplus C$.*

定理 7.56 *R-模 P 是投射的当且仅当 P 是一个自由 R-模的直和项．*

证明 假定 P 是投射模．根据命题 7.51，每个模都是自由模的商．于是存在自由模 F 和满射 $g: F \to P$，从而存在正合列

$$0 \to \ker g \to F \xrightarrow{g} P \to 0.$$

现在命题 7.54 表明 P 是 F 的直和项．

假设 P 是自由模 F 的直和项，从而存在映射 $q: F \to P$ 和 $j: P \to F$ 满足 $qj = 1_P$. 现在考虑图

$$\begin{array}{ccccc} F & \underset{j}{\overset{q}{\rightleftarrows}} & P & & \\ h\downarrow & & \downarrow f & & \\ B & \xrightarrow{p} & C & \longrightarrow & 0 \end{array}$$

其中 p 是满射．复合 fq 是映射 $F \to C$；因 F 是自由的，它必是投射的，从而存在映射 $h: F \to B$ 满足 $ph = fq$. 定义 $g: P \to B$ 为 $g = hj$. 剩下要证明 $pg = f$. 但

$$pg = phj = fqj = f1_P = f.$$ ■

事实上，这个证明的第二部分表明投射模的任意一个直和项也是投射的．

现在我们可以举出一个交换环 R 和一个不自由的投射 R-模的例子．

例 7.57 环 $R = \mathbb{I}_6$ 是两个理想的直和：

$$\mathbb{I}_6 = J \oplus I,$$

其中

$$J = \{[0],[2],[4]\} \cong \mathbb{I}_3 \text{ 和 } I = \{[0],[3]\} \cong \mathbb{I}_2.$$

现在 $\mathbb{I}_6$ 是它自身上的自由模，从而 I 和 J 作为自由模的直和项是投射 $\mathbb{I}_6$-模．然而 J 和 I 都不可能是自由的．毕竟一个（有限生成的）自由 $\mathbb{I}_6$-模 F 是若干个（比如 n 个）$\mathbb{I}_6$ 的复制的直和，从而 F 有 6^n 个元素．所以 J 太小从而不能成为自由模，因为它只有三个元素． ■

476

描述投射 R-模的问题深深依赖于环 R. 例如在第 9 章中，我们将证明如果 R 是 PID，则自由模的每个子模也是自由的．此时会从定理 7.56 推出每个投射 R-模是自由的．一个高难度的结果是：如果 $R = k[x_1, \cdots, x_n]$ 是域 k 上 n 个变量的多项式环，则每个投射 R-模都是自由的. 关于这个定理，塞尔先提出猜测[⊖]，奎伦(D. Quillen) 和苏斯林(A. Suslin) 独立地给出了证明（证明见罗特曼所著的《An

---

⊖ "Faisceaux Algèbriques Cohérents" 243 页，*Annals of Mathematics* 61 (1955)，197～278，塞尔写道："…on ignore s'il existe des A-modules projectifs de type fini qui ne soient pas libres." 这里 $A = k[x_1, \cdots, x_n]$.

Introduction to Homological Algebra》138～145页). N. Fitchas, A. Galligo和B. Sturmfels有一个奎伦-苏斯林定理的证明，该证明用到了格罗布纳基．

存在这样的整环，它有不自由的投射模．例如 R 是一个代数数域（即 $\mathbb{Q}$ 的次数有限的扩张）中一切代数整数的环，则 R 中的每个理想都是投射 R-模．还存在这样的环 R，它不是 PID，R 中的任一非主理想都是不自由的投射模(在第 11 章中讨论戴德金环时将看到这个结果).

这里是投射模的另一种刻画．注意，如果 A 是具有基 $\{a_i : i\in I\}\subseteq A$ 的自由 R-模，则每个 $x\in A$ 有唯一的表达式 $x=\sum_{i\in I} r_i a_i$，从而存在由 $\varphi_i : x\mapsto r_i$ 给出的 R-映射 $\varphi_i : A\to R$．

命题 7.58 *R-模 A 是投射模当且仅当存在元素 $\{a_i : i\in I\}\subseteq A$ 和 R-映射 $\{\varphi_i : A\to R : i\in I\}$ 满足*

(ⅰ) 对每个 $x\in A$，几乎一切 $\varphi_i(x)=0$；

(ⅱ) 对每个 $x\in A$，有 $x=\sum_{i\in I}(\varphi_i x)a_i$．

此外，在这种情形中 $\{a_i : i\in I\}\subseteq A$ 生成 A．

证明 如果 A 是投射模，则存在自由 R-模 F 和满射 R-映射 $\psi: F\to A$．因 A 是投射的，根据命题 7.54，存在 R-映射 $\varphi: A\to F$ 使得 $\psi\varphi=1_A$. 设 $\{e_i : i\in I\}$ 是 F 的基，定义 $a_i=\psi(e_i)$．现在，如果 $x\in A$，则存在唯一表达式 $\varphi(x)=\sum_i r_i e_i$，其中 $r_i\in R$ 且几乎一切 $r_i=0$．定义 $\varphi_i : A\to R$ 为 $\varphi_i(x)=r_i$. 当然，给定 x，对几乎一切 i 有 $\varphi_i(x)=0$. 因 ψ 是满射，A 由 $\{a_i=\psi(e_i) : i\in I\}$ 生成．最后，

$$\begin{aligned}x=\psi\varphi(x)&=\psi(\sum r_i e_i)\\&=\sum r_i\psi(e_i)=\sum(\varphi_i x)\psi(e_i)=\sum(\varphi_i x)a_i.\end{aligned}$$

反之，如命题陈述中那样给定 $\{a_i : i\in I\}\subseteq A$ 和一族 R-映射 $\{\varphi_i : A\to R : i\in I\}$，定义 F 是以 $\{e_i : i\in I\}$ 为基的自由 R-模，定义 R-映射 $\psi: F\to A$ 为 $\psi: e_i\mapsto a_i$. 现在只需找到一个 R-映射 $\varphi: A\to F$ 使得 $\psi\varphi=1_A$，因为由此可推出 A 是（同构于）一个收缩核（即 A 是 F 的直和项），因此 A 是投射模．定义 φ 为 $\varphi(x)=\sum_i(\varphi_i x)e_i$，其中 $x\in A$．根据条件（ⅰ），这个和是有限的，从而 φ 是合理定义的．根据条件（ⅱ），

477

$$\psi\varphi(x)=\psi\sum(\varphi_i x)e_i=\sum(\varphi_i x)\psi(e_i)=\sum(\varphi_i x)a_i=x;$$

即 $\psi\varphi=1_A$. ■

定义 如果 A 是 R-模，则满足命题 7.58 中的条件的子集 $\{a_i : i\in I\}\subseteq A$ 和一族 R-映射 $\{\varphi_i : A\to R : i\in I\}$ 叫做**投射基**．

投射基有一个属于 R. Bkouche 的有趣应用．设 X 是一个局部紧豪斯多夫空间，设 $C(X)$ 是 X 上一切连续实值函数的环，并设 J 是由一切具有紧支撑的函数组成的 $C(X)$ 中的理想，则 X 是仿紧空间当且仅当 J 是投射 $C(X)$-模．

注 如果能够把满射翻译为范畴的语言，那么投射模的定义可以用来定义任意范畴中的投射对象（我们并没有声称这种对象一定存在）．习题 7.18 产生一个候选者，但我们现在将看到在任意范畴中定义满射并不是十分简单的．

定义 称范畴 $\mathcal{C}$ 中的一个态射 $\varphi: B\to C$ 为**满态射**，如果 φ 可以右消去，即对一切对象 D 和一

切态射 $h: C \to D, k: C \to D$，有 $h\varphi = k\varphi$ 蕴涵 $h = k$.

$$B \xrightarrow{\varphi} C \underset{k}{\overset{h}{\rightrightarrows}} D$$

现在习题 7.18 证明 $_R$**Mod** 范畴中的满态射就是满射，习题 7.45 和习题 7.19 分别证明在集合范畴和群范畴中的满态射也是满射．然而，在交换环范畴中，易知如果 R 是整环，则由 $r \mapsto 1/r$ 给出的环同态 $\varphi: R \to \mathrm{Frac}(R)$ 是范畴中的满态射．如果 A 是交换环，$h, k: \mathrm{Frac}(R) \to A$ 是在 R 上一致的环同态，则 $h = k$．但当 R 不是域时，φ 就不是满射函数．类似的现象出现在 **Top** 范畴中．如果 $f: X \to Y$ 是连续映射且 $\mathrm{im} f$ 是 Y 的稠密子空间，则 f 是满态射，这是因为任意两个连续函数在一个稠密子空间上一致必相等．

单射推广到任意范畴中的**单态射**也有类似的问题：一个范畴中有底集的对象可以有单态射，但它的底函数不是单射． ■

我们回到模的表现．

478

定义 称 R-模 M 是**有限表现的**，如果它有表现 $(\mathcal{X} \mid \mathcal{R})$，其中 X 和 $\mathcal{R}$ 都是有限的．

如果 M 是有限表现的，则存在短正合列

$$0 \to K \to F \to M \to 0,$$

其中 F 是自由的，K 和 F 都是有限生成的．等价地说，M 是有 限表现的，如果存在正合列

$$F' \to F \to M \to 0,$$

其中 F' 和 F 都是有限生成的自由模(就是把一个有限生成的自由模 F' 映射到 K 上)．注意第二个正合列不以"$0 \to$" 起首．

命题 7.59 如果 R 是交换诺特环，则每个有限生成 R-模都是有限表现的．

证明 如果 M 是有限生成 R-模，则存在有限生成自由 R-模 F 和满射 $\varphi: F \to M$. 因 R 是诺特环，命题 7.23 说 F 的每个子模都是有限生成的．特别地，$\ker\varphi$ 是有限生成的，因此 M 是有限表现的． ■

每个有限表现模都是有限生成的，但我们立刻会看到逆命题可能不成立．先比较一个模的两个表现（我们稍作推广，把自由模换成投射模）．

命题 7.60 (Schanuel 引理) 给定正合列

$$0 \to K \xrightarrow{i} P \xrightarrow{\pi} M \to 0$$

和

$$0 \to K' \xrightarrow{i'} P' \xrightarrow{\pi'} M \to 0,$$

其中 P 和 P' 是投射模，则存在同构

$$K \oplus P' \cong K' \oplus P.$$

证明 考虑行正合的图

$$\begin{array}{ccccccccc} 0 & \to & K & \xrightarrow{i} & P & \xrightarrow{\pi} & M & \to & 0 \\ & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle 1_M} & & \\ 0 & \to & K' & \xrightarrow{i'} & P' & \xrightarrow{\pi'} & M & \to & 0 \end{array}$$

因 P 是投射的，存在映射 $\beta: P \to P'$ 使得 $\pi'\beta = \pi$；即图中右边的正方形交换．我们现在证明存在映

射 $\alpha: K \to K'$ 使得其他的正方形交换．如果 $x \in K$，则因 $\pi i = 0$ 有 $\pi'\beta ix = \pi ix = 0$. 因此 $\beta ix \in \ker\pi' = \operatorname{im} i'$，于是存在 $x' \in K'$ 使得 $i'x' = \beta x$；此外，因 i' 是单射，从而 x' 唯一．所以 $\alpha: x \mapsto x'$ 是合理定义的函数 $\alpha: K \to K'$,它使得第一个正方形交换．读者可以证明 α 是 R-映射． 479

这个有两个正合行的交换图给出一个正合列

$$0 \to K \xrightarrow{\theta} P \oplus K' \xrightarrow{\psi} P' \to 0,$$

其中 $\theta: x \mapsto (ix, \alpha x)$ 和 $\psi: (u, x') \mapsto \beta u - i'x'$,其中 $x \in K, u \in P, x' \in K'$. 这个序列的正合性只需简单计算,留给读者. 因 P' 是投射模，所以这个序列是分裂的． ■

系 7.61 如果 M 是有限表现的且

$$0 \to K \to F \to M \to 0$$

是正合列，其中 F 是有限生成自由模,则 K 是有限生成的.

证明 因 M 是有限表现的，存在正合列

$$0 \to K' \to F' \to M \to 0,$$

其中 F' 是自由的，F' 和 K' 都是有限生成的．根据 Schanuel 引理，$K \oplus F' \cong K' \oplus F$．现在因为 $K' \oplus F$ 的两个直和项都是有限生成的，所以 $K' \oplus F$ 是有限生成的，从而左端也是有限生成的．但直和项 K 是 $K \oplus F'$ 的同态象，因此它是有限生成的． ■

我们现在给出一个不是有限表现的有限生成模的例子．

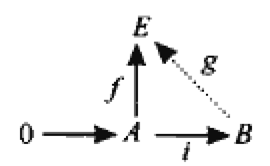
例 7.62 设 R 是非诺特交换环,即 R 包含一个不是有限生成的理想（见例 6.39）．我们断言 R-模 $M = R/I$ 是有限生成的，但不是有限表现的．当然，M 是有限生成的，它甚至是循环的．如果 M 是有限表现的，则有正合列 $0 \to K \to F \to M \to 0$,其中 F 是自由的,K 和 F 都是有限生成的．和系 7.61 一样，把它和正合列 $0 \to I \to R \to M \to 0$ 比较,得出 I 是有限生成的，产生矛盾．所以 M 不是有限表现的． ■

还有另一种类型的模也是重要的．

定义 如果 E 是模，反变 Hom 函子 $\operatorname{Hom}_R(\ ,E)$ 是正合函子，即 $\operatorname{Hom}_R(\ ,E)$ 保持一切短正合列，则称 E 为 **内射模**．

下一命题是命题 7.53 的对偶． 480

命题 7.63 模 E 是内射模当且仅当只要 i 是单射就存在一个虚线箭头使得下图交换：



用文字来说，一个子模到 E 中的每个同态恒可扩张为从一个大的模到 E 中的同态．

注 因 $\operatorname{Hom}_R(\ ,E)$ 是左正合反变函子，所以这个命题的核心是只要 i 是单射，i^* 便是满射．用图来刻画时，内射模是投射模的对偶，内射性的图就是反转投射性图的一切箭头．

证明 如果 E 是内射模,则 $\operatorname{Hom}(\ ,E)$ 是正合函子，从而 i^* 是满射．所以，如果 $f \in \operatorname{Hom}_R(A,E)$，则存在 $g \in \operatorname{Hom}_R(B,E)$ 使得 $f = i^*(g) = gi$；即图交换．

关于逆命题，如果 E 满足图条件，则给定 $f: A \to E$, 存在 $g: B \to E$ 使得 $gi = f$．于是，如果 $f \in \operatorname{Hom}_R(A,E)$，则 $f = gi = i^*(g) \in \operatorname{im} i^*$，由此 i^* 是满射．所以 $\operatorname{Hom}(\ ,E)$ 是正合函子，从而 E 是内射模． ■

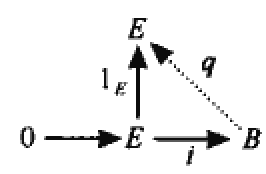
下一结果是命题 7.54 的对偶．

命题 7.64 模 E 是内射模当且仅当每个短正合列

$$0 \to E \xrightarrow{i} B \xrightarrow{p} C \to 0$$

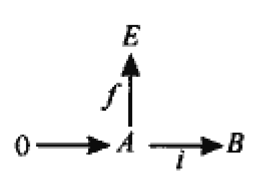
都是分裂的.

证明 如果 E 是内射模,则存在 $q: B \to E$ 使得下图交换,即 $qi = 1_E$.



现在习题 7.17 给出结果.

反之，假定每个以 E 开始的正合列分裂. 图



481

的推出是图

$$\begin{array}{ccccc} & & E & \xrightarrow{\alpha} & D \\ & & f\uparrow & & \uparrow\beta \\ 0 & \longrightarrow & A & \xrightarrow{i} & B \end{array}$$

根据习题 7.28，映射 α 是单射，从而

$$0 \to E \to D \to \operatorname{coker}\alpha \to 0$$

分裂；即存在 $q: D \to E$ 满足 $q\alpha = 1_E$. 如果定义 $g: B \to E$ 为 $g = q\beta$，则原始图交换：

$$gi = q\beta i = q\alpha f = 1_E f = f.$$

所以 E 是内射模. ■

这个命题可以不用正合这个词重新叙述.

系 7.65 如果内射模 E 是一个模 M 的子模,则 E 是 M 的直和项:存在 M 的子模 S 使得 $S \cong M/E$ 和 $M = E \oplus S$.

命题 7.66 如果 $\{E_i : i \in I\}$ 是一族内射模,则 $\prod_{i\in I} E_i$ 也是内射模.

证明 考虑图

$$\begin{array}{ccccc} & & E & & \\ & & f\uparrow & & \\ 0 & \longrightarrow & A & \xrightarrow{\kappa} & B \end{array}$$

其中 $E = \prod E_i$. 设 $p_i: E \to E_i$ 是第 i 个投射. 因 E_i 是内射模,存在 $g_i: B \to E_i$ 使得 $g_i\kappa = p_i f$. 现在定义 $g: B \to E$ 为 $g: b \mapsto (g_i(b))$. 如果 $b = \kappa a$,则映射 g 扩张 f，于是

$$g(\kappa a) = (g_i(\kappa a)) = (p_i f a) = fa,$$

这是因为 $x = (p_i x)$ 对乘积中的每个 x 成立. ■

系 7.67 内射模的有限直和是内射模.

证明 有限个模的直和与直积相同. ■

482

下面白尔的定理是一个十分有用的结果.

定理 7.68 (白尔判别法) R-模 E 是内射模当且仅当每个 R-映射 $f: I \to E$ 都可以扩张到 R 上,其中 I 是 R 中的理想.

$$\begin{array}{ccccc} & & E & & \\ & & f\uparrow & \nwarrow g & \\ 0 & \to & I & \xrightarrow{i} & R \end{array}$$

证明 因任一理想 I 都是 R 的子模，所以 f 的一个扩张 g 的存在性正是 E 的内射性定义的特殊情形.

假设有图

$$\begin{array}{ccccc} & & E & & \\ & & f\uparrow & & \\ 0 & \to & A & \xrightarrow{i} & B \end{array}$$

其中 A 是模 B 的子模. 为了记号的方便，假定 i 是包含映射［这个假定等于允许把 $i(a)$ 写作 a，只要 $a \in A$］. 我们要用附录中的佐恩引理来扩张 f. 精确地说，设 X 是一切有序对 (A', g') 的集合，其中 $A \subseteq A' \subseteq B$ 和 $g' : A' \to E$ 扩张 f；即 $g' \mid A = f$. 注意，因 $(A, f) \in X$，所以 $X \neq \varnothing$. 定义 X 上的偏序

$$(A', g') \leq (A'', g'')$$

为 $A' \subseteq A''$ 且 g'' 扩张 g'. 读者可以补充适用佐恩引理的论证，因此在 X 中存在极大元素 (A_0, g_0). 如果 $A_0 = B$，结论已经得到，因此可以假定有某个 $b \in B$ 使得 $b \notin A_0$.

定义

$$I = \{r \in R : rb \in A_0\}.$$

易知 I 是 R 中的理想. 定义 $h : I \to E$ 为

$$h(r) = g_0(rb).$$

根据假设，存在映射 $h^* : R \to E$ 扩张 h. 最后，定义 $A_1 = A_0 + \langle b \rangle$ 和 $g_1 : A_1 \to E$ 为

$$g_1(a_0 + rb) = g_0(a_0) + rh^*(1),$$

其中 $a_0 \in A_0$ 和 $r \in R$.

我们证明 g_1 是合理定义的. 如果 $a_0 + rb = a'_0 + r'b$，则 $(r - r')b = a'_0 - a_0 \in A_0$，由此 $r - r' \in I$. 所以 $g_0((r - r')b)$ 和 $h(r - r')$ 有定义，且有

$$g_0(a'_0 - a_0) = g_0((r - r')b) = h(r - r') = h^*(r - r') = (r - r')h^*(1).$$

于是，如所要求的，$g_0(a'_0) - g_0(a_0) = rh^*(1) - r'h^*(1)$ 和 $g_0(a'_0) + r'h^*(1) = g_0(a_0) + rh^*(1)$. 显然对一切 $a_0 \in A_0$ 有 $g_1(a_0) = g_0(a_0)$，从而映射 g_1 扩张 g_0. 由此推出 $(A_0, g_0) \prec (A_1, g_1)$，与 (A_0, g_0) 的极大性矛盾. 所以 $A_0 = B$，映射 g_0 是 f 的提升，E 是内射模. ■ [483]

内射模的任意直和是内射模吗?

命题 7.69 如果 R 是诺特环，$\{E_i : i \in I\}$ 是一族内射 R-模，则 $\sum_{i \in I} E_i$ 是内射模.

证明 根据定理 7.68，即白尔判别法，只需完成图

$$\begin{array}{ccccc} & & \sum_{i \in I} E_i & & \\ & & f\uparrow & & \\ 0 & \to & J & \xrightarrow{\kappa} & R \end{array}$$

其中 J 是 R 中的理想. 因 R 是诺特环，所以 J 是有限生成的，比如 $J = (a_1, \cdots, a_n)$. 对 $k = 1, \cdots, n$，$f(a_k) \in \sum_{i \in I} E_i$，只有有限个非零坐标，比如它们出现在一个指标集 $S(a_k) \subseteq I$ 中. 于是 $S = \bigcup_{k=1}^{n} S(a_k)$ 是有限集，且 $\operatorname{im} f \subseteq \sum_{i \in S} E_i$；根据系 7.67，这个有限和是内射模. 因此存在 R-映射 $g' : R$

$\to \sum_{i\in S} E_i$ 扩张 f. 把 g' 和 $\sum_{i\in S} E_i$ 到 $\sum_{i\in I} E_i$ 的包含映射复合起来就可完成给定的图. ■

巴斯 (H. Bass) 的一个定理证明命题 7.69 的逆命题成立：如果内射 R-模的每个直和都是内射模，则 R 是诺特环（见定理 8.105）.

我们现在可以给出内射模的几个例子.

命题 7.70 *如果 R 是整环，则 $Q = \text{Frac}(R)$ 是内射 R-模.*

证明 根据白尔判别法，只需把一个 R-映射 $f: I \to Q$ 扩张到整个 R，其中 I 是 R 中的理想. 首先注意，如果 $a,b \in I$ 是非零元素，则 $af(b) = f(ab) = bf(a)$，因此

$$\text{对一切非零 } a,b \in I, \text{在 } Q \text{ 中有 } f(a)/a = f(b)/b,$$

令 $c \in Q$ 表示它们共同的值（注意，为定义 c，要求 I 是理想：积 ab 必须有定义，且每个因子都可拿到括号外面）. 定义 $g: R \to Q$ 为对一切 $r \in R$，

$$g(r) = rc.$$

显然 g 是 R-映射. 为证明 g 扩张 f，假设 $a \in I$，则

$$g(a) = ac = af(a)/a = f(a).$$

现在由白尔判别法，Q 是内射 R-模. ■

定义 *如果 R 是整环，则称一个 R-模 D 是**可除的**，如果对每个 $d \in D$ 和每个非零 $r \in R$，存在 $d' \in D$ 使得 $d = rd'$.*

484

例 7.71 设 R 是整环.

(i) $\text{Frac}(R)$ 是可除 R-模.

(ii) 可除 R-模的每个直和是可除的. 因此，$\text{Frac}(R)$ 上的每个向量空间是可除 R-模.

(iii) 每个可除 R-模的商是可除的. ■

引理 7.72 *如果 R 是整环，则每个内射 R-模 E 都是可除的.*

证明 假定 E 是内射模. 设 $e \in E$ 和 $r_0 \in R$ 是非零元素；我们必须求出 $x \in E$ 使得 $e = r_0x$. 定义 $f: (r_0) \to E$ 为 $f(rr_0) = re$（注意 f 是合理定义的：因 R 是整环，$rr_0 = r'r_0$ 蕴涵 $r = r'$）. 因 E 是内射模，存在 $h: R \to E$ 扩张 f. 特别地，

$$e = f(r_0) = h(r_0) = r_0h(1),$$

因此 $x = h(1)$ 就是可除性定义所要求的 E 中的元素. ■

我们现在证明对 PID，引理 7.72 的逆成立. 命题 11.111 证明整环 R 是戴德金环（在最后一章定义）当且仅当每个可除 R-模是内射模.

系 7.73 *如果 R 是 PID，则 R-模 E 是内射模当且仅当它是可除模.*

证明 假定 E 是可除的. 根据定理 7.68，即白尔判别法，只要把映射 $f: I \to E$ 扩张到整个 R. 因 R 是 PID，所以 I 是主理想，比如 $I = (r_0)$，其中 $r_0 \in I$. 因 E 是可除的，存在 $e \in E$ 使得 $r_0e = f(r_0)$. 定义 $h: R \to E$ 为 $h(r) = re$. 易知 h 是扩张 f 的 R-映射，因此 E 是内射模. ■

注 *存在可除模不是内射模的整环；事实上，存在内射模的商未必是内射模的整环.*

例 7.74 依据例 7.71，下面的阿贝尔群都是内射 $\mathbb{Z}$-模：

$$\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}/\mathbb{Z}, \mathbb{R}/\mathbb{Z}, S^1,$$

其中 S^1 是圆群，即 $|z| = 1$ 的一切复数 z 的乘法群. ■

命题 7.51 说，在任意环上，每个模都是投射模的商（事实上，有更强的结果：每个模都是自由模的商）. 下一结果是关于 $\mathbb{Z}$-模的对偶结果：每个阿贝尔群可以作为子群嵌入一个内射阿贝尔

群．我们将在第 8 章中对任意环上的模证明这个结果（见定理 8.104）． [485]

系 7.75 每个阿贝尔群 M 可以作为子群嵌入某个内射阿贝尔群．

证明 根据命题 7.51，存在自由阿贝尔群 $F=\sum_i \mathbb{Z}_i$ 使得对某个 $K\subseteq F$ 有 $M=F/K$．现在

$$M=F/K=\Big(\sum_i \mathbb{Z}_i\Big)/K\subseteq\Big(\sum_i \mathbb{Q}_i\Big)/K,$$

其中我们只是把 $\mathbb{Z}$ 的每个复制 $\mathbb{Z}_i$ 嵌入到 $\mathbb{Q}$ 的一个复制 $\mathbb{Q}_i$．但例 7.71 给出每个 $\mathbb{Q}_i$ 可除，因此给出 $\sum_i \mathbb{Q}_i$ 可除，并因此给出商 $\big(\sum_i \mathbb{Q}_i\big)/K$ 的可除性．根据系 7.73，$\big(\sum_i \mathbb{Q}_i\big)/K$ 是内射的． ■

把一个模写作自由模的商本质上是用生成元和关系描述它．可以把上面的系看作这个观点的对偶．

下一结果给出内射模的一个古怪的例子，事实上，我们将用它来证明一个重要结果（见 654 页基定理证明之后的注）．

命题 7.76 设 R 是 PID，$a\in R$ 既不是零也不是单位，并设 $J=(a)$，则 R/J 是内射 R/J-模．

证明 根据对应定理，R/J 中的每个理想形如 I/J，其中 I 是 R 中包含 J 的某个理想．现在有某个 $b\in I$ 使得 $I=(b)$，因此 I/J 是循环的，它具有生成元 $x=b+J$．因 $(a)\subseteq(b)$，所以对某个 $r\in R$ 有 $a=rb$．我们将用定理 7.68，即白尔判别法来证明 R/J 是内射的．

假定 $f: I/J\to R/J$ 是 R/J-映射，记 $f(b+J)=s+J$，其中 $s\in R$．因 $r(b+J)=rb+J=a+J=0$，有 $rf(b+J)=r(s+J)=rs+J=0$，从而 $rs\in J=(a)$．因此存在某个 $r'\in R$ 使得 $rs=r'a=r'br$；消去 r 得 $s=r'b$．于是

$$f(b+J)=s+J=r'b+J.$$

定义 $h: R/J\to R/J$ 为乘 r'，即 $h: u+J\mapsto r'u+J$．上面的等式给出 $h(b+J)=f(b+J)$，从而 h 扩张 f．所以 R/J 是内射的． ■

习题

7.40 设 M 是自由 R-模，其中 R 是整环．证明：如果 $rm=0$，其中 $r\in R$ 和 $m\in M$，则或者 $r=0$，或者 $m=0$．（R 不是整环则不成立．）

7.41 用 Hom 的左正合性证明：如果 G 是阿贝尔群，则 $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{I}_n,G)\cong G[n]$，其中 $G[n]=\{g\in G: ng=0\}$．

7.42 证明群 $G\in\mathrm{obj}$(群范畴)是一个投射对象当且仅当 G 是自由群．（习题 10.3 中证明在群范畴中唯一的内射对象是 $\{1\}$．） [486]

7.43 如果 R 是整环但不是域，且 $Q=\mathrm{Frac}(R)$，证明

$$\mathrm{Hom}_R(Q,R)=\{0\}.$$

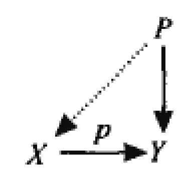
7.44 证明每个左正合共变函子 $T: {}_R\mathbf{Mod}\to\mathbf{Ab}$ 保持拉回．由此推出：如果 B 和 C 是模 A 的子模，则对每个模 M 有

$$\mathrm{Hom}_R(M,B\cap C)=\mathrm{Hom}_R(M,B)\cap\mathrm{Hom}_R(M,C).$$

提示：用拉回．

7.45 （i）证明一个函数是集合范畴中的满态射当且仅当它是满射．

（ii）证明集合范畴中的每个对象都是投射的，一个范畴中的对象 P 是投射的，如果对于图



恒有虚线箭头，其中 p 是一个满态射．

提示：用选择公理．

7.46 给定集合 X，证明存在这样的自由 R-模 F，它的基 B 有一个双射 $\varphi: B \to X$.

7.47 (ⅰ) 证明域 k 上的每个向量空间 V 都是自由 k-模．

(ⅱ) 证明 V 的子集 B 是把 V 看作向量空间时的基当且仅当 B 是把 V 看作自由 k-模时的基．

7.48 定义 G 是有表现 $(\mathcal{X} \mid \mathcal{R})$ 的阿贝尔群，其中

$$\mathcal{X} = \{a, b_1, b_2, \cdots, b_n, \cdots\} \text{ 和 } \mathcal{R} = \{2a, a - 2^n b_n, n \geqslant 1\}.$$

于是，$G = F/K$，其中 F 是以$\mathcal{X}$为基的自由阿贝尔群，K 是子群$\langle \mathcal{R} \rangle$．

(ⅰ) 证明 $a + K \in G$ 是非零元素．

(ⅱ) 证明 $z = a + K$ 满足等式 $z = 2^n y_n$，其中 $y_n \in G$ 且 $n \geqslant 1$，并证明 z 是 G 中唯一这样的元素．

(ⅲ) 证明存在正合列$0 \to \langle a \rangle \to G \to \sum_{n \geqslant 1} \mathbb{I}_{2^n} \to 0$.

(ⅳ) 把 $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \ )$ 作用到(ⅲ)中的正合列上，以此证明 $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, G) = \{0\}$.

7.49 (ⅰ) 如果$\{P_i : i \in I\}$是一族投射 R-模，证明它们的直和$\sum_{i \in I} P_i$ 也是投射的．

(ⅱ) 证明投射模的每个直和项也是投射模．

7.50 证明内射模的每个直和项也是内射模．

7.51 举出一个模的例子，它的两个内射子模的交不是内射模．

提示：定义阿贝尔群 $A \cong \mathbb{Z}(p^\infty) \cong A'$：

$$A = (a_n, n \geqslant 0 \mid pa_0 = 0, pa_{n+1} = a_n) \text{ 和 } A' = (a'_n, n \geqslant 0 \mid pa'_0 = 0, pa'_{n+1} = a'_n).$$

487

在 $A \oplus A'$ 中定义 $E = A \oplus \{0\}$ 和 $E' = \langle \{(a_{n+1}, a'_n) : n \geqslant 0\} \rangle$.

7.52 (ⅰ) 证明：如果整环 R 是内射 R-模，则 R 是域．

(ⅱ) 设 R 是整环但不是域，并设 R-模 M 既是内射的又是投射的．证明 $M = \{0\}$.

(ⅲ) 证明$\mathbb{I}_6$ 既是它自身上的内射模又是它自身上的投射模．

7.53 (ⅰ) 如果 R 是整环，且 I 和 J 都是R 中的非零理想，证明 $I \cap J \neq \{0\}$.

(ⅱ) 设 R 是整环，并设 R 中的理想 I 是自由 R-模，证明 I 是主理想．

7.54 (ⅰ) 证明 R-模 E 是内射模当且仅当对 R 中的每个理想 I，每个短正合列$0 \to E \to B \to I \to 0$分裂．

(ⅱ) 如果 R 是整环，证明无挠可除 R-模是内射的.

7.55 证明 Schanuel 引理的对偶．给定正合列

$$0 \to M \xrightarrow{i} E \xrightarrow{p} Q \to 0 \text{ 和 } 0 \to M \xrightarrow{i'} E' \xrightarrow{p'} Q' \to 0,$$

其中 E 和 E'都是内射模，则存在同构

$$Q \oplus E' \cong Q' \oplus E.$$

7.56 (ⅰ) 证明域 k 上的每个向量空间都是内射 k-模．

(ⅱ) 证明：如果 $0 \to U \to V \to W \to 0$ 是向量空间的正合列，则对偶空间的对应序列 $0 \to W^* \to V^* \to U^* \to 0$ 也是正合列．

7.57 (**庞特里亚金对偶性**) 如果 G 是阿贝尔群，它的**庞特里亚金对偶** (Pontrjagin) 是指群

$$G^* = \mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{Q}/\mathbb{Z}).$$

(庞特里亚金对偶性可以扩张到局部紧阿贝尔拓扑群，对偶由映入圆群的一切连续同态组成.)

(ⅰ) 证明：如果 G 是阿贝尔群且 $a \in G$ 是非零元素，则存在同态 $f: G \to \mathbb{Q}/\mathbb{Z}$ 满足 $f(a) \neq 0$.

(ii) 证明$\mathbb{Q}/\mathbb{Z}$是内射阿贝尔群.

(iii) 证明:如果$0\to A\to G\to B\to 0$是阿贝尔群的正合列,则$0\to B^*\to G^*\to A^*\to 0$也是阿贝尔群的正合列.

(iv) 如果$G\cong \mathbb{I}_n$,证明$G^*\cong G$.

(v) 如果G是有限阿贝尔群,证明$G^*\cong G$.

(vi) 证明:如果G是有限阿贝尔群,且G/H是G的商群,则G/H同构于G的一个子群.[类似的陈述对非阿贝尔群不成立:如果$\mathbf{Q}$是四元数群,则$\mathbf{Q}/Z(\mathbf{Q})\cong \mathbf{V}$,其中$\mathbf{V}$是四群.但$\mathbf{Q}$只有一个2阶元素,而$\mathbf{V}$有三个2阶元素.这个习题对无限阿贝尔群也不成立:因$\mathbb{Z}$没有2阶元素,所以它没有子群能够同构于$\mathbb{Z}/2\mathbb{Z}\cong\mathbb{I}_2$.]

7.5 格罗滕迪克群

格罗滕迪克引入阿贝尔群以帮助研究投射模.读者可以把本节看作代数K-理论的一个平易的介绍.

488

定义 范畴$\mathcal{C}$称为$\star$-范畴,如果存在交换和结合的二元运算$\star$:$\text{obj}(\mathcal{C})\times\text{obj}(\mathcal{C})\to\text{obj}(\mathcal{C})$;即

(i) 如果$A\cong A'$和$B\cong B'$,其中$A,A',B,B'\in\text{obj}(\mathcal{C})$,则$A\star B\cong A'\star B'$.

(ii) 对一切$A,B\in\text{obj}(\mathcal{C})$,存在等价$A\star B\cong B\star A$.

(iii) 对一切$A,B,C\in\text{obj}(\mathcal{C})$,存在等价$A\star(B\star C)\cong(A\star B)\star C$.

有有限积或有有限余积的范畴是$\star$-范畴.

定义 如果$\mathcal{C}$是$\star$-范畴,定义$|\text{obj}(\mathcal{C})|$为$\mathcal{C}$中对象的一切同构类$|A|$的类,其中$|A|=\{B\in\text{obj}(\mathcal{C}):B\cong A\}$.如果$\mathcal{F}(\mathcal{C})$是这样的自由阿贝尔群,它的基[⊖]为$|\text{obj}(\mathcal{C})|$,$\mathcal{R}$是由形如

$$|A\star B|-|A|-|B|,\text{其中 }A,B\in\text{obj}(\mathcal{C})$$

的一切元素生成的$\mathcal{F}(\mathcal{C})$的子群,则**格罗滕迪克群**$K_0(\mathcal{C})$是指阿贝尔群

$$K_0(\mathcal{C})=\mathcal{F}(\mathcal{C})/\mathcal{R}.$$

(习题7.58中给出$K_0(\mathcal{C})$作为泛映射问题的解的一个刻画.)对$\mathcal{C}$中的任意对象A,记陪集$|A|+\mathcal{R}$为$[A]$.

我们说明格罗滕迪克群$K_0(\mathcal{C})$能够定义得更确切:$\mathcal{C}$应该是对称单项范畴(见Mac Lane所著的《Categories for the Working Mathematician》,157~161页).

命题7.77 设$\mathcal{C}$是$\star$-范畴.

(i) 如果$x\in K_0(\mathcal{C})$,则有$A,B\in\text{obj}(\mathcal{C})$,使得$x=[A]-[B]$.

(ii) 如果$A,B\in\text{obj}(\mathcal{C})$,则在$K_0(\mathcal{C})$中$[A]=[B]$当且仅当存在$C\in\text{obj}(\mathcal{C})$使得$A\star C\cong B\star C$.

证明 (i) 因$K_0(\mathcal{C})$由$|\text{obj}(\mathcal{C})|$生成,可记

$$x=\sum_{i=1}^{r}[A_i]-\sum_{j=1}^{s}[B_j].$$

(允许对象A_i和B_i可以重复.)现在如果定义$A=A_1\star\cdots\star A_r$,则

$$[A]=[A_1\star\cdots\star A_r]=\sum_i[A_i].$$

同样,定义$B=B_1\star\cdots\star B_s$.显然$x=[A]-[B]$.

489

⊖ 这里有集合论的一个小问题,因为自由阿贝尔群的基必须是一个集合而不是一个真类,为避免这个问题常假定$\mathcal{C}$是一个小范畴,即类$\text{obj}(\mathcal{C})$是集合.

(ⅱ) 如果 $A\star C\cong B\star C$,则在 $K_0(\mathcal{C})$ 中 $[A\star C]=[B\star C]$. 因此 $[A]+[C]=[B]+[C]$,阿贝尔群 $K_0(\mathcal{C})$ 中的消去律给出 $[A]=[B]$.

反之,如果 $[A]=[B]$,则 $|B|-|A|\in\mathcal{R}$,且在 $\mathcal{F}(\mathcal{C})$ 中有等式

$$|B|-|A|=\sum_i m_i(|X_i\star Y_i|-|X_i|-|Y_i|)-\sum_j n_j(|U_j\star V_j|-|U_j|-|V_j|),$$

其中系数 m_i 和 n_j 都是正整数,X,Y,U,V 都是 $\mathcal{C}$ 中的对象.移项消去负系数得

$$|A|+\sum_i m_i|X_i\star Y_i|+\sum_j n_j(|U_j|+|V_j|)=|B|+\sum_i m_i(|X_i|+|Y_i|)+\sum_j n_j|U_j\star V_j|.$$

这是自由阿贝尔群中的等式,用基来表达是唯一的.所以,左端对象的集合 $\{A,X_i\star Y_i,U_j,V_j\}$ 连同重数和右端对象的集合 $\{B,U_j\star V_j,X_i,Y_i\}$ 连同重数是一样的.因积是交换和结合的,在 $\mathcal{C}$ 中有等价:

$$A\star(\bigstar_i m_i(X_i\star Y_i))\star(\bigstar_j n_j(U_j\star V_j))\cong B\star(\bigstar_i m_i(X_i\star Y_i))\star(\bigstar_j n_j(U_j\star V_j)).$$

检查这些项表明

$$(\bigstar_i m_i(X_i\star Y_i))\star(\bigstar_j n_j(U_j\star V_j))\cong(\bigstar_i m_i(X_i\star Y_i))\star(\bigstar_j n_j(U_j\star V_j)).$$

如果记最后这个对象为 C,则 $A\star C\cong B\star C$. ■

定义 设 R 是交换环,并设 $\mathcal{C}$ 是 ${}_R\mathbf{Mod}$ 的子范畴.称两个 R-模 A 和 B **在 $\mathcal{C}$ 中稳定同构**,如果存在模 $C\in obj(\mathcal{C})$ 满足 $A\oplus C\cong B\oplus C$.

用这个术语,命题 7.77 说明两个模确定格罗滕迪克群中的同一元素当且仅当它们是稳定同构的.显然,同构的模是稳定同构的,下例表明逆不成立.

例 7.78 (ⅰ) 如果 **Ab** 是一切有限阿贝尔群的范畴,则习题 5.10 表明两个有限阿贝尔群在 **Ab** 中稳定同构当且仅当它们是同构的.

(ⅱ) 如果 R 是交换环,F 是秩无限的自由 R-模,则

490

$$R\oplus F\cong R\oplus R\oplus F.$$

于是模 R 和 $R\oplus R$ 不同构,但在 ${}_R\mathbf{Mod}$ 中稳定同构.鉴于这种类型的例子,我们常把自己限制在有限生成模组成的 ${}_R\mathbf{Mod}$ 的子范畴 $\mathcal{C}$ 中.

(ⅲ) 这里是 R. G. Swan 的一个例子,其中有限生成投射模的稳定同构不蕴涵同构.

设 $R=\mathbb{R}[x_1,\cdots,x_n]/(1-\sum_i x_i^2)$[实 $(n-1)$-球面的坐标环].把 R^n 看作 $n\times 1$ 列向量,并设 $X=(\overline{x}_1,\cdots,\overline{x}_n)^t\in R^n$,其中横线表示 R 中 $\mathrm{mod}(1-\sum_i x_i^2)$ 的陪集.定义 $\lambda:R\to R^n$ 为 $\lambda:r\mapsto rX$,并定义 $\varphi:R^n\to R$ 为 $\varphi(Y)=X^tY$.注意复合 $\varphi\lambda:R\to R$ 是恒等映射,这是因为 $X^tX=\sum_i\overline{x}_i^2=1$,从而

$$\varphi\lambda(r)=\varphi(rX)=X^trX=r.$$

由此,正合列

$$0\to R\xrightarrow{\lambda}R^n\xrightarrow{\text{自然映射}}R^n/\mathrm{im}\lambda\to 0$$

分裂.于是,如果 $P=R^n/\mathrm{im}\lambda$,则

$$R\oplus R^{n-1}\cong R^n\cong R\oplus P,$$

从而 P 稳定同构于自由 R-模 R^{n-1}(当然,P 是投射 R-模).Swan 用拓扑证明了 P 是自由 R-模当且仅当 $n=1,2,4,8$.例如,如果 $n=3$,P 就不同构于 R^{n-1}. ■

命题 7.79 如果 $\mathcal{C}$ 是一切有限阿贝尔群的范畴,则 $K_0(\mathcal{C})$ 是自由阿贝尔群,一切准素循环群组成它的基 $\mathcal{B}$.

证明 由基定理，每个有限阿贝尔群 $A \cong \sum_i C_i$，其中 C_i 是准素循环群．于是在 $K_0(\mathcal{C})$ 中 $[A]=\sum_i [C_i]$．因对 $K_0(\mathcal{C})$ 中的每个元素存在有限阿贝尔群 A,B 使它等于 $[A]-[B]$，因此 $\mathcal{B}$ 生成 $K_0(\mathcal{C})$．为证明 $\mathcal{B}$ 是基，假设 $\sum_{i=1}^{r} m_i[C_i]-\sum_{j=1}^{s} n_j[C'_j]=0$，其中 m_i 和 n_j 是正整数．则 $\sum_i [m_iC_i]=\sum_j [n_jC'_j]$，其中 m_iC_i 是 m_i 个 C_i 的复制的直和，从而 $\left[\sum_i m_iC_i\right]=\left[\sum_j n_jC'_j\right]$．所以在 $\mathcal{C}$ 中 $\sum_i m_iC_i$ 和 $\sum_j n_jC'_j$ 稳定同构．根据例 7.78(i)，$\sum_{i=1}^{r} m_iC_i \cong \sum_{j=1}^{s} n_jC'_j$．最后运用有限阿贝尔群的基本定理得 $r=s$，并存在置换 $\sigma \in S_r$ 使得对一切 i，$C'_{\sigma(i)} \cong C_i$ 和 $m_i=n_{\sigma(i)}$．所以 $\mathcal{B}$ 是 $K_0(\mathcal{C})$ 的基． ■

定义 如果 R 是交换环，则一切有限生成投射 R-模的子范畴 $\mathbf{Pr}(R)$ 是 $\star$-范畴（因为两个有限生成投射 R-模的直和还是有限生成投射 R-模）．此时我们常记 $K_0(\mathbf{Pr}(R))$ 为 $K_0(R)$． [491]

例 7.80 我们现在证明：如果 R 是交换环，且对于这个 R，每个有限生成投射 R-模都是自由的，则 $K_0(R)\cong\mathbb{Z}$．显然 $K_0(R)$ 由 $[R]$ 生成，因此 $K_0(R)$ 是循环群．定义 $r: \mathrm{obj}(\mathbf{Pr}(R))\to\mathbb{Z}$ 为 $r(F)=\mathrm{rank}(F)$，其中 F 是有限生成自由 R-模．因 $r(F\oplus F')=r(F)+r(F')$，习题 7.58 证明对每个有限生成自由 R-模 F 有满足 $\tilde{r}([F])=\mathrm{rank}(F)$ 的同态 $\tilde{r}: K_0(R)\to\mathbb{Z}$．因 $K_0(R)$ 是循环群，$\tilde{r}$ 是同构．

如果 $\mathcal{C}$ 是模范畴，我们可以定义另一个格罗滕迪克群 $K'(\mathcal{C})$． ■

定义 如果 $\mathcal{C}$ 是模范畴，定义 $\mathcal{F}(\mathcal{C})$ 为这样的自由阿贝尔群，它的基为 $|\mathrm{obj}(\mathcal{C})|$，$\mathcal{R}$ 为由一切形如

$$|B|-|A|-|C|，\text{如果存在正合列 } 0\to A\to B\to C\to 0$$

的元素生成的 $\mathcal{F}(\mathcal{C})$ 的子群．**格罗滕迪克群** $K'(\mathcal{C})$ 是指阿贝尔群

$$K'(\mathcal{C})=\mathcal{F}(\mathcal{C})/\mathcal{R}'；$$

即 $K'(\mathcal{C})$ 是有生成元 $|\mathrm{obj}(\mathcal{C})|$ 和关系 $\mathcal{R}'$ 的阿贝尔群．对任一模 $A\in\mathrm{obj}(\mathcal{C})$，我们记陪集 $|A|+\mathcal{R}'$ 为 (A)．

例 7.81 如果 R 是整环且 $a\in R$ 既不是 0 也不是单位，则存在正合列

$$0\to R\xrightarrow{\mu_a}R\to R/Ra\to 0,$$

其中 $\mu_a: r\mapsto ar$．于是在 $K'(\mathcal{C})$ 中有等式：

$$(R)=(R)+(R/Ra).$$

因此，$(R/Ra)=0$． ■

下一命题用来考察格罗滕迪克群的两个概念—— $K_0(R)=K_0(\mathbf{Pr}(R))$ 和 $K'(\mathbf{Pr}(R))$ —— 的一致性．理由是存在正合列 $0\to A\to A\oplus C\to C\to 0$，因此在 $K'(\mathcal{C})$ 中有 $(A\oplus C)=(A)+(C)$．

命题 7.82 如果 R 是交换环，$\mathcal{C}$ 是一切有限生成 R-模的范畴，则存在同态

$$\varepsilon: K_0(R)\to K'(\mathcal{C}),$$

其中对每个投射 R-模 P，$\varepsilon: [P]\mapsto(P)$．

证明 因投射模的每个短正合列分裂，定义 $K_0(R)=K_0(\mathbf{Pr}(R))$ 的关系和定义 $K'(\mathbf{Pr}(R))$ 的关系是相同的．因此包含映射 $\mathcal{F}(\mathbf{Pr}(R))\to\mathcal{F}(\mathcal{C})$ 诱导出一个合理定义的同态． ■ [492]

命题 7.83 设 R 是交换环，$\mathcal{C}$ 是一切有限生成 R-模的范畴．如果 $M\in\mathrm{obj}(\mathcal{C})$ 和

$$M=M_0\supseteq M_1\supseteq M_2\supseteq\cdots\supseteq M_n=\{0\}$$

有因子模 $Q_i = M_{i-1}/M_i$，则

$$\text{在 } K'(\mathcal{C}) \text{ 中}, (M) = (Q_1) + \cdots + (Q_n).$$

证明 因 $Q_i = M_{i-1}/M_i$，存在短正合列

$$0 \to M_i \to M_{i-1} \to Q_i \to 0,$$

因此在 $K'(\mathcal{C})$ 中有 $(Q_i) = (M_{i-1}) - (M_i)$. 现在我们有重叠和：

$$\sum_{i=1}^{n}(Q_i) = \sum_{i=1}^{n}[(M_{i-1}) - (M_i)] = (M_0) - (M_n) = (M). \quad \blacksquare$$

下面一个明显的问题是如何发现 $K'(\mathcal{C})$ 中的一个元素何时是零.

命题 7.84 设 R 是交换环，$\mathcal{C}$是一切有限生成 R-模的范畴. 如果 $A, B \in \text{obj}(\mathcal{C})$，则在 $K'(\mathcal{C})$ 中 $(A) = (B)$ 当且仅当存在 $C, U, V \in \text{obj}(\mathcal{C})$ 和正合列

$$0 \to U \to A \oplus C \to V \to 0 \quad \text{和} \quad 0 \to U \to B \oplus C \to V \to 0.$$

证明 如果像命题陈述中那样存在模 C，U 和 V，则

$$(A \oplus C) = (U) + (V) = (B \oplus C).$$

但 $0 \to A \to A \oplus C \to C \to 0$ 的正合性给出 $(A \oplus C) = (A) + (C)$. 同样，$(B \oplus C) = (B) + (C)$，因此 $(A) + (C) = (B) + (C)$ 和$(A) = (B)$.

反之，如果 $(A) = (B)$，则 $|A| - |B| \in \mathcal{R}'$. 和命题 7.77 的证明一样，在 $\mathcal{F}(\mathcal{C})$ 中有等式：

$$|A| + \sum |X_i| + \sum(|Y_j'| + |Y_j''|) = |B| + \sum(|X_i'| + |X_i''|) + \sum |Y_j|,$$

其中 $0 \to X_i' \to X_i \to X_i'' \to 0$ 和 $0 \to Y_j' \to Y_j \to Y_j'' \to 0$ 都是正合列. 定义

$$C = A \oplus \sum X_i \oplus \sum (Y_j' \oplus Y_j'').$$

令 X' 为 X_i' 的直和，X 为 X_i 的直和，等等，命题 7.77 证明中的论证给出

$$A \oplus X \oplus Y' \oplus Y'' \cong B \oplus X' \oplus X'' \oplus Y.$$

493

根据习题 7.12，这个同构产生正合列

$$0 \to X' \oplus Y'' \to X \oplus Y'' \to X'' \to 0,$$

$$0 \to X' \oplus Y'' \to (X \oplus Y'') \oplus Y' \to X'' \oplus Y' \to 0$$

和

$$0 \to X' \oplus Y'' \to A \oplus (X \oplus Y' \oplus Y'') \to A \oplus (X'' \oplus Y') \to 0.$$

中间模是 C. 再次运用习题 7.12，存在正合列

$$0 \to X' \oplus Y' \to B \oplus C \to B \oplus (A \oplus X'' \oplus Y'') \to 0.$$

定义 $U = X' \oplus Y'$ 和 $V = B \oplus A \oplus X'' \oplus Y''$，使用这个记号，最后的正合列是

$$0 \to U \to B \oplus C \to V \to 0.$$

同样的处理产生正合列 $0 \to U \to A \oplus C \to V \to 0$. $\blacksquare$

第 8 章中我们将证明定理 5.52 即若尔当-赫尔德定理的模版本. 而现在仅给出一个定义.

定义 称模范畴$\mathcal{C}$中的序列

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots \supseteq M_n = \{0\}$$

为 M 的**合成列**，如果它的每个因子模 $Q_i = M_{i-1}/M_i$ 都是 $\text{obj}(\mathcal{C})$ 中的单模. 我们称模范畴$\mathcal{C}$是**若尔当-赫尔德范畴**，如果：

（i）每个对象 M 都有合成列；

（ii）对每两个合成列

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots \supseteq M_n = \{0\}$$

和

$$M = M'_0 \supseteq M'_1 \supseteq M'_2 \supseteq \cdots \supseteq M'_m = \{0\},$$

有 $m = n$ 和置换 $\sigma \in S_n$ 使得对一切 j 有 $Q'_j \cong Q_{\sigma j}$，其中 $Q_i = M_{i-1}/M_i$ 和 $Q'_j = M'_{j-1}/M'_j$.

定义若尔当-赫尔德范畴中模 M 的**长度** $\ell(M)$ 为合成列中项的个数 n. 如果合成列的因子单模是 $Q_1, \cdots, Q_n$，我们定义

$$\text{jh}(M) = Q_1 \oplus \cdots \oplus Q_n.$$

一个合成列可以有几个同构的因子模，jh(M) 记录它们的重数．

494

引理 7.85 设$\mathcal{C}$是若尔当-赫尔德范畴，并设 $Q_1, \cdots, Q_n, Q'_1, \cdots, Q'_m$ 都是 obj$(\mathcal{C})$ 中的单模．

（ⅰ）如果

$$Q_1 \oplus \cdots \oplus Q_n \cong Q'_1 \oplus \cdots \oplus Q'_m,$$

则 $m = n$ 且有置换 $\sigma \in S_n$ 使得对一切 j 有 $Q'_j \cong Q_{\sigma j}$，其中 $Q_i = M_{i-1}/M_i$ 和 $Q'_j = M'_{j-1}/M'_j$.

（ⅱ）如果 M 和 M' 都是 obj$(\mathcal{C})$ 中的模，且存在单模 $S \in$ obj$(\mathcal{C})$ 使得

$$S \oplus \text{jh}(M) \cong S \oplus \text{jh}(M'),$$

则 jh$(M) \cong$ jh(M').

证明 （ⅰ）现在

$$Q_1 \oplus \cdots \oplus Q_n \supseteq Q_2 \oplus \cdots \oplus Q_n \supseteq Q_3 \oplus \cdots \oplus Q_n \supseteq \cdots$$

是因子模为 $Q_1, \cdots, Q_n$ 的合成列，同样，同构模 $Q'_1 \oplus \cdots \oplus Q'_m$ 是有因子模 $Q'_1, \cdots, Q'_m$ 的合成列．由$\mathcal{C}$是若尔当-赫尔德范畴可得结论．

（ⅱ）因 S 是单模，从（ⅰ）可得结论． ■

引理 7.86 如果 $0 \to A \to B \to C \to 0$ 是若尔当-赫尔德范畴中的正合列，则

$$\text{jh}(B) \cong \text{jh}(A) \oplus \text{jh}(C).$$

证明 对长度 $\ell(C)$ 用归纳法证明．设 $A = A_0 \supseteq A_1 \supseteq \cdots \supseteq A_n = \{0\}$ 是 A 的合成列，它的因子模是 $Q_1, \cdots, Q_n$. 如果 $\ell(C) = 1$，则 C 是单模，因此

$$B \supseteq A \supseteq A_1 \supseteq \cdots \supseteq A_n = \{0\}$$

是 B 的合成列，它的因子模是 $C, Q_1, \cdots, Q_n$. 所以

$$\text{jh}(B) = C \oplus Q_1 \oplus \cdots \oplus Q_n = \text{jh}(C) \oplus \text{jh}(A).$$

关于归纳步，设 $\ell(C) > 1$. 选取 C 的极大子模 C_1（因为 C 有合成列，所以极大子模存在）．如果 $v: B \to C$ 是给定的满射，定义 $B_1 = v^{-1}(C_1)$．有交换图（垂直箭头是包含映射）

$$\begin{array}{ccccccccc} 0 & \to & A & \to & B & \xrightarrow{v} & C & \to & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \to & A & \to & B_1 & \to & C_1 & \to & 0 \end{array}$$

495

因 C_1 是 C 的极大子模，所以商模

$$C'' = C/C_1$$

是单模．注意 $B/B_1 \cong (B/A)/(B_1/A) \cong C/C_1 = C''$. 根据基础步，有

$$\text{jh}(C) = C'' \oplus \text{jh}(C_1) \quad \text{和} \quad \text{jh}(B) = C'' \oplus \text{jh}(B_1).$$

根据归纳假设，

$$\text{jh}(B_1) = \text{jh}(A) \oplus \text{jh}(C_1).$$

所以,

$$\begin{aligned}\mathrm{jh}(B) &= C'' \oplus \mathrm{jh}(B_1) \\ &\cong C'' \oplus \mathrm{jh}(A) \oplus \mathrm{jh}(C_1) \\ &\cong \mathrm{jh}(A) \oplus C'' \oplus \mathrm{jh}(C_1) \\ &\cong \mathrm{jh}(A) \oplus \mathrm{jh}(C).\end{aligned}$$

■

定理 7.87 设$\mathcal{C}$是模范畴，其中每个模 $M \in \mathrm{obj}(\mathcal{C})$ 都有合成列，则$\mathcal{C}$是若尔当-赫尔德范畴当且仅当 $K'(\mathcal{C})$ 是自由阿贝尔群，它的基 $\mathcal{B}'$ 由一切 (S) 组成，S 遍历 $\mathrm{obj}(\mathcal{C})$ 中一切不同构的单模.

证明 假定 $K'(\mathcal{C})$ 是以 $\mathcal{B}'$ 为基的自由阿贝尔群. 因 0 不是基的成员，对每个单模 S 有 $(S) \neq 0$. 此外，如果 $S \ncong S'$，则因基中没有重复的元素，所以 $(S) \neq (S')$. 设 $M \in \mathrm{obj}(\mathcal{C})$，并设 $Q_1, \cdots, Q_n$ 和 $Q'_1, \cdots, Q'_m$ 是单模，它们分别是 M 的两个合成列的因子模，根据命题 7.83，有

$$(Q_1) + \cdots + (Q_n) = (M) = (Q'_1) + \cdots + (Q'_m).$$

使用基$\mathcal{B}'$来表达的唯一性说明对每个 Q'_j，存在 Q_i 使得 $(Q_i) = (Q'_j)$；事实上，左端任一 (Q_i) 的个数等于右端 (Q'_j) 的复制的个数. 所以$\mathcal{C}$是若尔当-赫尔德范畴.

反之，假定对$\mathcal{C}$若尔当-赫尔德定理成立. 因每个 $M \in \mathrm{obj}(\mathcal{C})$ 都有合成列，命题 7.83 证明 $\mathcal{B}'$ 生成 $K'(\mathcal{C})$. 设 S 是 $\mathrm{obj}(\mathcal{C})$ 中的单模. 如果 $(S) = (T)$，则命题 7.84 说存在 $C, U, V \in \mathrm{obj}(\mathcal{C})$，以及正合列 $0 \to U \to S \oplus C \to V \to 0$ 和 $0 \to U \to T \oplus C \to V \to 0$. 引理 7.86 给出

$$\mathrm{jh}(S) \oplus \mathrm{jh}(C) \cong \mathrm{jh}(U) \oplus \mathrm{jh}(V) \cong \mathrm{jh}(T) \oplus \mathrm{jh}(C).$$

496

根据引理 7.85，我们可以逐个消去单直和项，直到留下 $S \cong T$. 同样的论证表明，如果 S 是单模，则 $(S) \neq 0$. 最后，我们证明 $K'(\mathcal{C})$ 中的每个元素作为 $\mathcal{B}'$ 中元素的线性组合的表达式唯一. 假设存在正整数 m_i 和 n_j 使得

$$\sum_i m_i(S_i) - \sum_j n_j(T_j) = 0, \tag{1}$$

其中 S_i 和 T_j 都是 $\mathrm{obj}(\mathcal{C})$ 中的单模，且对一切 $i, j, S_i \ncong T_j$. 如果记 S_i 的 m_i 个复制的直和为 m_iS_i，则等式 (1) 给出

$$\Big(\sum_i m_iS_i\Big) = \Big(\sum_j n_jT_j\Big).$$

根据命题 7.84，存在模 C，U，V 和正合列

$$0 \to U \to C \oplus \sum_i m_iS_i \to V \to 0 \text{ 和 } 0 \to U \to C \oplus \sum_j n_jT_j \to V \to 0,$$

并且引理 7.86 给出

$$\mathrm{jh}\Big(\sum_i m_iS_i\Big) \cong \mathrm{jh}\Big(\sum_j n_jT_j\Big).$$

根据引理 7.85，有某个 S_i 出现在右端，与对一切 $i, j, S_i \ncong T_j$ 矛盾. 所以等式 (1) 不可能出现. ■

注 称模 M 为**不可分解模**，如果不存在非零模 A 和 B 使得 $M \cong A \oplus B$. 我们说模范畴$\mathcal{C}$为**克鲁尔-施密特范畴**，如果

(i) $\mathrm{obj}(\mathcal{C})$ 中的每个模都同构于 $\mathrm{obj}(\mathcal{C})$ 中不可分解模的一个有限直和.

(ii) 如果

$$D_1 \oplus \cdots \oplus D_n \cong D'_1 \oplus \cdots \oplus D'_m,$$

其中一切直和项都是不可分解模，则 $m=n$，且存在置换 $\sigma\in S_n$ 使得对于一切 j 有 $D'_j\cong D_{\sigma j}$.

有一个类似于定理 7.87 的定理说：模范畴$\mathcal{C}$是克鲁尔-施密特范畴当且仅当 $K_0(\mathcal{C})$ 是自由阿贝尔群，它的基由一切 $[D]$ 组成，D 遍历 obj$(\mathcal{C})$中一切不同构的不可分解模.

把下一个系和命题 7.79 作比较.

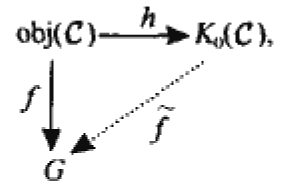
系 7.88 如果$\mathcal{C}$是一切有限阿贝尔群的范畴，则 $K'(\mathcal{C})$ 是自由阿贝尔群，它的生成元是一切 (S)，其中 S 是阶为素数 p 的循环群.

证明 根据定理 5.52，一切有限阿贝尔群的范畴是一个若尔当-赫尔德范畴，而单 Z-模是阿贝尔群 $\mathbb{I}_p$，其中 p 是素数. ■ 497

巴斯定义了更高的群 K_1 和 K_2，证明存在一个正合列把它们和 K_0 联系起来，并展示了如何用这些群来研究投射模.（见 Milnor 所著的《Introduction to Algebraic K-Theory》. 奎伦把一个拓扑空间 $X(\mathcal{C})$和某个范畴$\mathcal{C}$结合起来，从而构造了阿贝尔群的无穷序列 $K_n(\mathcal{C})$. 然后他对一切 $n\geqslant 0$ 定义了$K_n(\mathcal{C})=\pi_{n+1}(X(\mathcal{C}))$；即这个空间的同伦群，并证明他的 K_n 和巴斯的那些在 $n=0,1,2$ 时相同（见 Rosenberg 所著的《Algebraic K-theory and Its Applications》.

习题

7.58 设$\mathcal{C}$是$\star$-范畴. 证明 $K_0(\mathcal{C})$ 解决了下面的泛映射问题.



其中 G 是任一阿贝尔群. 如果 $h:\text{obj}(\mathcal{C})\to K_0(\mathcal{C})$ 是函数 $A\mapsto[A]$，且 $f:\text{obj}(\mathcal{C})\to G$ 满足只要 $A\cong B$ 便有 $f(A)=f(B)$以及满足 $f(A\star B)=f(A)+f(B)$，则存在唯一的同态$\tilde{f}:K_0(\mathcal{C})\to G$ 使得图交换.

7.59 把$\mathcal{C}=\mathbf{PO}(\mathbb{N})$看作一个$\star$-范畴，其中，$m\star n=m+n$，证明 $K_0(\mathcal{C})\cong\mathbb{Z}$.（由此，我们已经从自然数构造出整数. 用类似的方法，可以从一个半群 S 构造一个阿贝尔群 G，尽管我们不能期望 S 总能嵌入 G.）

7.60 (i) 如果$\mathcal{C}$是一个模范畴，它的对象有无限直和，证明 $K_0(\mathcal{C})=\{0\}$.

(ii)（艾伦伯格）证明：如果 P 是投射R-模(在某个交换环 R 上)，则存在自由 R-模 Q 使得 $P\oplus Q$ 是自由 R-模. 由此推出，对可数生成投射 R-模的范畴$\mathcal{C}$有 $K_0(\mathcal{C})=\{0\}$.

提示：Q 不必是有限生成的.

7.61 证明 $K_0(\mathbb{I}_6)\cong\mathbb{Z}\oplus\mathbb{Z}$.

7.62 设$\mathcal{C}$和$\mathcal{C}'$都是$\star$-范畴，并设 $F:\mathcal{C}\to\mathcal{C}'$ 是$\star$-保持函子；即 $F(A\star B)\cong F(A)\star F(B)$. 证明 F 由 $[A]\mapsto[FA]$ 诱导出一个同态 $K_0(\mathcal{C})\to K_0(\mathcal{C}')$.

7.63 如果$\mathcal{C}$是一个模范畴，证明 $K'(\mathcal{C})$ 中的每个元素都有 $(A)-(B)$ 的形式，其中模 A,B 在 obj$(\mathcal{C})$ 中.

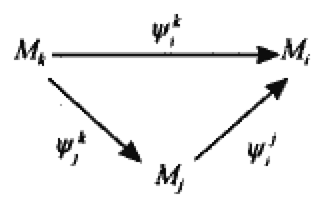
7.64 设$\mathcal{C}$是有短正合列的范畴. 证明存在满射 $K_0(\mathcal{C})\to K'(\mathcal{C})$.

7.6 极限

有两个更一般的结构，一个推广了拉回和交，另一个推广了推出和并，两者都牵涉到一族模 $\{M_i:i\in I\}$，它的指标集 I 是一个偏序集. 498

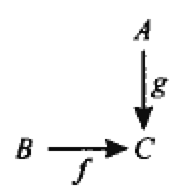
定义 设 I 是偏序集. I上R-模的**逆系统**是指有序对 $\{M_i,\psi_i^j\}$，它由模的一个加标族 $\{M_i:i\in I\}$ 和

对所有 $i \leq j$ 的一族态射 $\{\psi_i^j: M_j \to M_i\}$ 组成，使得对一切 i，$\psi_i^i = 1_{M_i}$，并当 $i \leq j \leq k$ 时下图交换：



例7.25(v)中，我们看到偏序集 I 定义了一个范畴 $\mathbf{PO}(I)$：$\mathbf{PO}(I)$ 的对象是 I 的元素，而 $\mathrm{Hom}(i,j)$ 当 $i \not\leq j$ 时是空集，当 $i \leq j$ 时只包含一个元素 κ_j^i. 如果定义 $F(i) = M_i$ 和 $F(\kappa_j^i) = \psi_i^j$，则易知 $\{M_i, \psi_i^j\}$ 是一个逆系统当且仅当 $F: \mathbf{PO}(I) \to {}_R\mathbf{Mod}$ 是一个反变函子. 现在我们看到可以定义涉及任意范畴$\mathcal{C}$中的对象和态射的逆系统：每个反变函子 $F: \mathbf{PO}(I) \to \mathcal{C}$ 产生一个. 例如我们可以谈论交换环的逆系统.

例 7.89 (i) 如果 $I = \{1,2,3\}$ 是有 $1 \leq 2$ 和 $1 \leq 3$ 的偏序集，则 I 上的一个逆系统是如下形式的图



(ii) 如果$\mathcal{I}$是模 A 的一族子模，则它能够在反包含关系下形成偏序集；即当 $M \supseteq M'$ 时 $M \leq M'$. 对 $M \leq M'$，包含映射 $M' \to M$ 有定义，易知一切 $M \in \mathcal{I}$ 的族连同包含映射是一个逆系统.

(iii) 如果 I 配置了离散偏序，即 $i \leq j$ 当且仅当 $i = j$，则 I 上的一个逆系统就是模的加标族.

(iv) 如果$\mathbb{N}$ 是具有通常偏序的自然数的集合，则$\mathbb{N}$ 上的一个逆系统是图

$$M_0 \leftarrow M_1 \leftarrow M_2 \leftarrow \cdots.$$

(v) 如果 J 是交换环 R 中的理想，则定义它的 n 次幂为

[499]

$$J^n = \{\sum a_1 \cdots a_n : a_i \in J\}.$$

每个 J^n 都是一个理想且有递减序列

$$R \supseteq J \supseteq J^2 \supseteq J^3 \supseteq \cdots.$$

如果 A 是 R-模，则存在子模序列

$$A \supseteq JA \supseteq J^2A \supseteq J^3A \supseteq \cdots.$$

如果 $m \geqslant n$，定义 $\psi_n^m: A/J^mA \to A/J^nA$ 为

$$\psi_n^m: a + J^mA \mapsto a + J^nA$$

(因为 $m \geqslant n$ 蕴涵 $J^mA \subseteq J^nA$，这些映射是合理定义的). 易知

$$\{A/J^nA, \psi_n^m\}$$

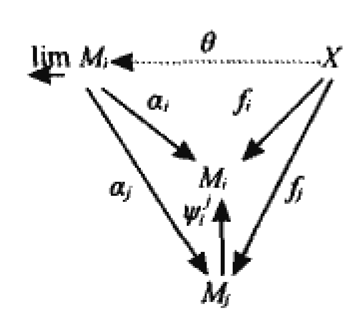
是$\mathbb{N}$ 上的一个逆系统.

(vi) 设 G 是群，并设$\mathcal{N}$是 G 的一切具有有限指数的正规子群的族，配置反包含关系的偏序，如果在 $\mathcal{N}$ 中 $N \leq N'$，则 $N' \leqslant N$. 定义 $\psi_N^{N'}: G/N' \to G/N$ 为 $gN' \mapsto gN$. 易知一切这种商的族连同映射 $\psi_N^{N'}$ 形成 $\mathcal{N}$ 上的一个逆系统. ■

定义 设 I 是偏序集，并设 $\{M_i, \psi_i^j\}$ 是 I 上 R-模的逆系统. **反向极限**（也叫做**投射极限**或**极限**）是指一个 R-模 $\varprojlim M_i$ 和一族 R-映射 $\{\alpha_i: \varprojlim M_i \to M_i : i \in I\}$，满足

(i) 只要 $i \leq j$ 就有 $\psi_i^j \alpha_j = \alpha_i$；

（ⅱ）对每个模 X 有映射 $f_i: X \to M_i$，且对一切 $i \leq j$ 满足 $\psi_i^j f_j = f_i$，并存在唯一的映射 $\theta: X \to \varprojlim M_i$ 使得下图交换：



反向极限的记号 $\varprojlim M_i$ 是不完全的，它没有反映相应的逆系统的映射（而 $\varprojlim M_i$ 依赖于它），然而这是通常的用法．

和作为泛映射问题的解定义的任一对象一样，一个逆系统的反向极限如果存在就是唯一的（不计同构）．

500

命题 7.90 存在偏序指标集 I 上的 R-模的任意一个逆系统 $\{M_i, \psi_i^j\}$ 的反向极限．

证明 定义

$$L = \{(m_i) \in \prod M_i : 只要 i \leq j 就有 m_i = \psi_i^j(m_j)\}.$$

容易验证 L 是 $\prod_i M_i$ 的子模．如果 p_i 是 $\prod_i M_i$ 到 M_i 的投射，定义 $\alpha_i: L \to M_i$ 为限制 $p_i \mid L$. 显然 $\psi_i^j \alpha_j = \alpha_i$.

假定 X 是一个模，它有映射 $f_i: X \to M_i$ 对一切 $i \leq j$ 满足 $\psi_i^j f_j = f_i$. 定义 $\theta: X \to \prod M_i$ 为

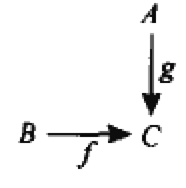
$$\theta(x) = (f_i(x)).$$

对一切 $i \leq j$，由给定的等式 $\psi_i^j f_j = f_i$ 可知 $\mathrm{im}\theta \subseteq L$. 而且，$\theta$ 使得图交换：$\alpha_i\theta: x \mapsto (f_i(x)) \mapsto f_i(x)$. 最后，$\theta$ 是唯一的映射 $X \to L$ 使得对于一切 $i \leq j$ 图交换．如果 $\varphi: X \to L$，则 $\varphi(x) = (m_i)$ 和 $\alpha_i \varphi(x) = m_i$. 于是，如果 φ 对一切 i 和一切 x 满足 $\alpha_i \varphi(x) = f_i(x)$，则 $m_i = f_i(x)$，从而 $\varphi = \theta$. 由此可知 $L \cong \varprojlim M_i$． ■

反向极限在不是模范畴的其他范畴中也可能存在，例如存在交换环的反向极限，群和拓扑空间的反向极限也存在．

读者应验证下面的论断，其中我们描述了例 7.89 中的各个逆系统的反向极限．

例 7.91 （ⅰ）如果 I 是满足 $1 \succeq 3$ 和 $2 \succeq 3$ 的偏序集 $\{1,2,3\}$，则一个逆系统是图



反向极限是拉回．

（ⅱ）我们已经看到一个模的两个子模的交是拉回的一个特殊情形．现在假设 $\mathcal{I}$ 是模 A 的一族子模，从而和例7.89（ⅱ）一样，$\mathcal{I}$ 和包含映射是一个逆系统．这个逆系统的反向极限是 $\bigcap_{M \in \mathcal{I}} M$.

（ⅲ）如果 I 是离散指标集，则逆系统 $\{M_i : i \in I\}$ 以积 $\prod_i M_i$ 为它的反向极限．其实，这正是积的图定义．

（ⅳ）如果 J 是交换环 R 中的理想，且 M 是一个 R-模，则 $\{M/J^n M, \psi_n^m\}$ ［例7.89（ⅴ）］的反

501 向极限常叫做M的J—**进位完备化**，我们把它记为$\hat{M}$. 为了理解这个术语，我们扫视点集拓扑的一角. ■

定义 **度量空间**是指一个集合X配置以叫做**度量**的函数$d: X\times X\to\mathbb{R}$，满足下列公理. 对一切$x,y,z\in X$，

（i）$d(x,y)\geqslant 0$，且$d(x,y)=0$当且仅当$x=y$；

（ii）$d(x,y)=d(y,x)$；

（iii）**（三角不等式）**$d(x,y)\leqslant d(x,z)+d(z,y)$.

例如，$d(x,y)=|x-y|$是$\mathbb{R}$上的一个度量. 给定度量空间X，序列收敛的通常定义有意义：X中点x_n的序列(x_n)叫做**收敛**到**极限**$y\in X$，如果对每个$\epsilon>0$，存在N使得只要$n\geqslant N$就有$d(x_n, y)<\epsilon$. 我们记(x_n)收敛到y为

$$x_n\to y.$$

这个定义的一个困难是不知道一个序列的极限是什么就不能谈到它收敛. 一个序列(x_n)称为**柯西序列**，如果对每个$\epsilon>0$存在N使得只要$m,n\geqslant N$就有$d(x_m,x_n)<\epsilon$. 关于序列的这个条件的优点是只涉及序列的项而不涉及它的极限. 如果$X=\mathbb{R}$，则一个序列收敛当且仅当它是一个柯西序列. 然而在一般的度量空间中，我们能够证明收敛序列是柯西序列，但反过来不成立. 例如X由一切正实数组成，它有通常的度量$|x-y|$，则序列$(1/n)$是柯西序列，但它在X中不收敛，因为$0\notin X$.

定义 度量空间X的**完备化**$\hat{X}$是指具有下列两个性质的度量空间：

（i）X是$\hat{X}$的稠密子空间，即对每个$\hat{x}\in\hat{X}$，存在X中的序列(x_n)使得$x_n\to\hat{x}$；

（ii）$\hat{X}$中的每个柯西序列收敛到$\hat{X}$中的一个极限.

可以证明度量空间X的任意两个完备化都是等距的（它们之间存在保持距离的双射），证明$\hat{X}$存在的一种方法是定义它的元素为X中柯西序列(x_n)的等价类，等价$(x_n)\equiv(y_n)$的定义是$d(x_n, y_n)\to 0$.

我们回到逆系统$\{M/J^nM,\psi_n^m\}$. 一个序列

$$(a_1+JM, a_2+J^2M, a_3+J^3M,\cdots)\in\varprojlim(M/J^nM)$$

满足条件：对一切$m\geqslant n, a_n+J^nM=\psi_n^m(a_m+J^mM)=a_m+J^nM$，从而

$$\text{只要 } m\geqslant n \text{ 就有 } a_m-a_n\in J^nM.$$

由此，在$\bigcap_{n=1}^{\infty}J^nM=\{0\}$的（特别重要的）特殊情形下，提出下面一种$M$上的度量. 如果$x\in M$且$x\neq 0$，则存在$i$使得$x\in J^iM$且$x\notin J^{i+1}M$. 定义$\|x\|=2^{-i}$，定义$\|0\|=0$. 经简单计算可知

502 $d(x,y)=\|x-y\|$是M上的度量（没有交条件，对一个非零$x\in\bigcap_{n=1}^{\infty}J^nM$，$\|x\|$可能没有定义）. 此外，如果$M$中的一个序列$(a_n)$是柯西序列，则$(a_1+JM,a_2+J^2M,a_3+J^3M,\cdots)\in\varprojlim M/J^nM$，使用子序列，可以看出实际上逆命题也成立.

特别是当$M=\mathbb{Z}$和$J=(p)$时，其中p是素数，完备化$\mathbb{Z}_p$叫做p-**进位整数环**. 由此，$\mathbb{Z}_p$是整环，$\mathbb{Q}_p=\mathrm{Frac}(\mathbb{Z}_p)$叫做$p$-**进位数域**.

（iii）在例7.89(vi)中我们已经看到群G中一切指数有限的正规子群的族$\mathcal{N}$形成一个逆系统，这个系统的反向极限$\varprojlim G/N$叫做G的**投射有限完备化**，记为$\hat{G}$. 存在映射$G\to\hat{G}$，也就是$g\mapsto(gN)$，它是单射当且仅当G是**剩余有限的**；即$\bigcap_{N\in\mathcal{N}}N=\{1\}$. 例如，已知每个自由群是剩余有限的.

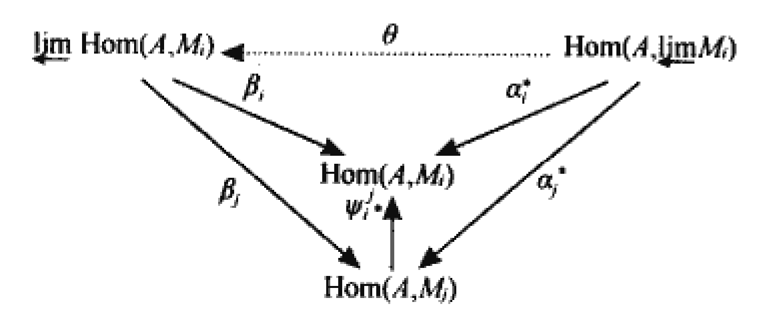
有一些使用投射有限完备化得到的有趣结果．如果 r 是一个正整数，称群 G 有秩 r，如果 G 的每个子群都可以由 r 个或少于 r 个元素生成．如果 G 是一个剩余有限 p-群（G 中每个元素的阶都是 p 的一个幂），它的秩为 r，则有某个 n 使得 G 同构于 $\mathrm{GL}(n,\mathbb{Z}_p)$ 的一个子群（不是每个剩余有限群都允许这样的线性嵌入）．见 Dixon-du Sautoy-Mann-Segal 所著的《Analytic Pro-p Groups》，98 页． ■

下一结果推广了定理 7.32.

命题 7.92 如果 $\{M_i,\psi_i^j\}$ 是逆系统，则对每个模 A，

$$\mathrm{Hom}(A,\varprojlim M_i)\cong\varprojlim\mathrm{Hom}(A,M_i).$$

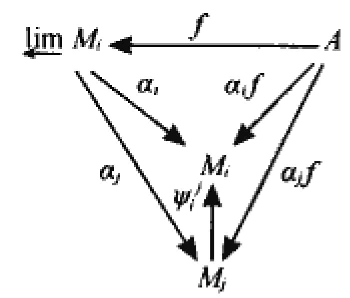
证明 由反向极限是泛映射问题的解可得结论．更详细地说，考虑图



其中 β_i 是反向极限定义中给出的映射．

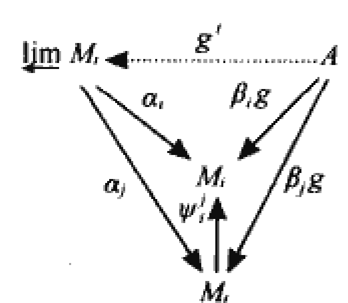
为证明 $\theta:\mathrm{Hom}(A,\varprojlim M_i)\to\varprojlim\mathrm{Hom}(A,M_i)$ 是单射，假设 $f:A\to\varprojlim M_i$ 和 $\theta(f)=0$. 则对一切 i, $0=\beta_i\theta f=\alpha_i f$，因此下图交换：

503



但替代 f 的零映射也使得图交换，因此这种映射的唯一性给出 $f=0$，即 θ 是单射．

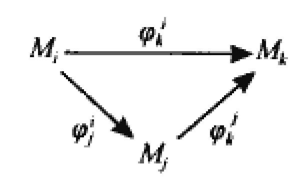
为证明 θ 是满射，取 $g\in\varprojlim\mathrm{Hom}(A,M_i)$. 对每个 i，有映射 $\beta_i g:A\to M_i$ 使得 $\psi_i^j\beta_i g=\beta_j g$.



$\varprojlim M_i$ 的定义对一切 i 提供映射 $g':A\to\varprojlim M_i$ 使得 $\alpha_i g'=\beta_i g$，由此，$g=\theta(g')$，即 θ 是满射. ■

现在我们考虑对偶结构．

定义 设 I 是偏序集．I 上的 R-模的**正系统**是指有序对 $\{M_i,\varphi_j^i\}$，它由模的一个加标族 $\{M_i:i\in I\}$ 和对所有 $i\le j$ 的一族态射 $\{\varphi_j^i:M_i\to M_j\}$ 组成，使得对一切 i，$\varphi_i^i=1_{M_i}$，并且只要 $i\le j\le k$，下图交换：



如果把 I 看作范畴 $\mathbf{PO}(I)$：当 $i \preceq j$ 时它只有态射 κ_j^i. 如果定义 $F(i) = M_i$ 和 $F(\kappa_j^i) = \varphi_j^i$，则易知 $\{M_i, \varphi_j^i\}$ 是一个正系统当且仅当 $F: \mathbf{PO}(I) \to {}_R\mathbf{Mod}$ 是一个（共变）函子. 于是，可以考虑涉及任意范畴$\mathcal{C}$中的对象和态射的正系统，而把这个正系统看作一个（共变）函子 $F: \mathbf{PO}(I) \to \mathcal{C}$. 例如，考虑交换环的正系统是有意义的.

504

例 7.93 （i）如果 $I = \{1,2,3\}$ 是 $1 \preceq 2$ 和 $1 \preceq 3$ 的偏序集，则 I 上的一个正系统是如下形式的图：

$$\begin{array}{ccc} A & \xrightarrow{g} & B \\ {\scriptstyle f}\downarrow & & \\ C & & \end{array}$$

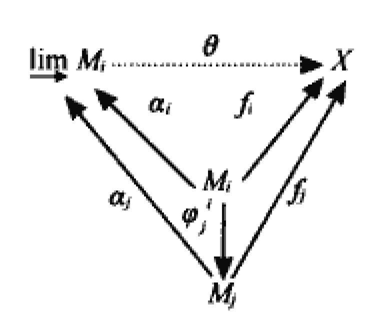
（ii）如果$\mathcal{I}$是模 A 的一族子模，则它可以形成包含关系下的偏序集，即当 $M \subseteq M'$ 时 $M \preceq M'$. 对 $M \preceq M'$，包含映射 $M \to M'$ 有定义，易知具有包含映射的一切 $M \in \mathcal{I}$ 的族是一个正系统.

（iii）如果 I 配置了离散偏序，则 I 上的一个正系统就是用 I 加标的一族模. ■

定义 设 I 是偏序集，并设 $\{M_i, \varphi_j^i\}$ 是 I 上 R-模的正系统. **正向极限**（也叫做**归纳极限**或**上极限**）是指一个 R-模 $\varinjlim M_i$ 和一族 R-映射 $\{\alpha_i: M_i \to \varinjlim M_i : i \in I\}$，满足

（i）只要 $i \preceq j$ 就有 $\alpha_j \varphi_j^i = \alpha_i$；

（ii）对每个有映射 $f_i: M_i \to X$ 的模 X，对一切 $i \preceq j$ 满足 $f_j \varphi_j^i = f_i$，且存在唯一的映射 θ：$\varinjlim M_i \to X$ 使得下图交换：



正向极限的记号 $\varinjlim M_i$ 是不完全的，它没有反映相应的正系统的映射（而 $\varinjlim M_i$ 依赖于它），然而这是通常的用法.

如同作为泛映射问题的解定义的任一对象一样，一个正系统的正向极限如果存在便是唯一的（不计同构）.

505

命题 7.94 存在偏序指标集 I 上任一 R-模的正系统 $\{M_i, \varphi_j^i\}$ 的正向极限.

证明 对每个 $i \in I$，设 λ_i 是 M_i 到和 $\sum_i M_i$ 中的内射. 定义

$$D = \left(\sum_i M_i\right)/S,$$

其中 S 是 $\sum_i M_i$ 的子模，它由一切元素 $\lambda_j \varphi_j^i m_i - \lambda_i m_i$ 生成，其中 $m_i \in M_i$ 和 $i \preceq j$. 现在定义 $\alpha_i: M_i \to D$ 为

$$\alpha_i: m_i \mapsto \lambda_i(m_i) + S.$$

容易验证 $D \cong \varinjlim M_i$. ■

由此，$\varinjlim M_i$ 的每个元素都可表示为 $\sum \lambda_i m_i + S$.

可以修改命题 7.94 中的论证用以证明其他范畴中存在正向极限，例如交换环、群和拓扑空间

都存在正向极限.

读者应验证下面的论断，其中我们描述了例 7.93 中若干正系统的正向极限，

例 7.95 （i）如果 I 是 $1 \leq 2$ 和 $1 \leq 3$ 的偏序集 $\{1,2,3\}$，则一个正系统是图

$$\begin{array}{ccc} A & \xrightarrow{g} & B \\ {\scriptstyle f}\downarrow & & \\ C & & \end{array}$$

正向极限是推出.

（ii）如果 I 是离散指标集，则正系统就是加标族 $\{M_i : i \in I\}$，正向极限是和：$\varinjlim M_i \cong \sum_i M_i$，这是因为在 $\varinjlim M_i$ 结构中的子模 S 是 $\{0\}$. 或者用另一种证法，这正是余积的图定义. ∎

下一结果推广了定理 7.33.

命题 7.96 如果 $\{M_i, \varphi_j^i\}$ 是一个正系统，则对每个模 B,

$$\mathrm{Hom}(\varinjlim M_i, B) \cong \varprojlim \mathrm{Hom}(M_i, B).$$

证明 由正向极限是泛映射问题的解可得结论. 这个证明是命题 7.92 的对偶，留给读者. ∎

有一种特殊的偏序指标集对正向极限有用.

[506]

定义 一个**有向集**是指偏序集 I，使得对每个 $i,j \in I$，存在 $k \in I$ 使得 $i \leq k$ 和 $j \leq k$.

例 7.97 （i）设$\mathcal{I}$是模 A 的子模的全序族；即如果 $M,M' \in \mathcal{I}$，则不是 $M \subseteq M'$ 就是 $M' \subseteq M$. 和例7.93(ii)一样，$\mathcal{I}$是偏序集，$\mathcal{I}$更是有向集.

（ii）如果 I 是有 $1 \leq 2$ 和 $1 \leq 3$ 的偏序集 $\{1,2,3\}$，则 I 不是有向集.

（iii）如果 $\{M_i : i \in I\}$ 是某个模的族，且 I 是离散偏序指标集，则 I 不是有向集. 然而，如果考虑一切有限部分和

$$M_{i_1} \oplus \cdots \oplus M_{i_n}$$

的族$\mathcal{F}$，则$\mathcal{F}$在包含关系下是有向集.

（iv）如果 A 是模，则和例7.93(ii)一样，A 的一切有限生成子模的族 $\mathrm{Fin}(A)$ 是包含关系下的偏序集，并且它还是有向集.

（v）如果 R是整环，$Q = \mathrm{Frac}(R)$，则和例7.93(ii)一样，Q 的一切形如 $\langle 1/r \rangle$ 的循环 R-子模的族是一个偏序集，其中 $r \in R$ 且 $r \neq 0$. 因为给定 $\langle 1/r \rangle$ 和 $\langle 1/s \rangle$，两者都包含在 $\langle 1/rs \rangle$ 之中，所以它是包含关系下的有向集.

（vi）设$\mathcal{U}$是$\mathbb{R}$ 中一切包含 0 的开区间的族，用反包含定义$\mathcal{U}$的偏序：

$$U \leq V \quad 如果 \quad V \subseteq U.$$

注意 $\mathcal{U}$ 是有向集：给定 $U,V \in \mathcal{U}$，则 $U \cap V \in \mathcal{U}$，从而 $U \leq U \cap V$ 和 $V \leq U \cap V$.

对每个 $U \in \mathcal{U}$，定义

$$\mathcal{F}(U) = \{f : U \to \mathbb{R} : f \text{ 是连续函数}\}.$$

如果 $U \leq V$，即 $V \subseteq U$，定义 $\rho_V^U : \mathcal{F}(U) \to \mathcal{F}(V)$ 为限制映射 $f \mapsto f \mid V$，则 $\{\mathcal{F}(U), \rho_V^U\}$ 是一个正系统. ∎

有两个理由考虑具有有向指标集的正系统. 第一个是正向极限中的元素可以有更简单的描述，第二个是 $\varinjlim$ 保持短正合列.

命题 7.98 设 $\{M_i, \varphi_j^i\}$ 是有向指标集 I 上左 R-模的正系统，并设 $\lambda_i : M_i \to \sum M_i$ 是第 i 个内

射，从而 $\varinjlim M_i = (\sum M_i)/S$，其中

$$S = \langle \lambda_j\varphi_j^i m_i - \lambda_i m_i : m_i \in M_i \text{ 和 } i \le j \rangle.$$

507

（i）$\varinjlim M_i$ 的每个元素都可表示为 $\lambda_i m_i + S$ 的形式（代替 $\sum_i \lambda_i m_i + S$）.

（ii）$\lambda_i m_i + S = 0$ 当且仅当有某个 $t \ge i$ 使得 $\varphi_t^i(m_i) = 0$.

证明 （i）和命题 7.94 的证明一样，正向极限存在，$\varinjlim M_i = (\sum M_i)/S$，因此一个典型元素 $x \in \varinjlim M_i$ 有 $x = \sum \lambda_i m_i + S$ 的形式. 因 I 是有向集，存在指标 j 使得对出现在 x 的和式中的一切 i 有 $j \ge i$. 对每个这样的 i 定义 $b^i = \varphi_j^i m_i \in M_j$，从而由 $b = \sum_i b^i$ 定义的元素 b 在 M_j 中. 由此，

$$\begin{aligned}\sum\lambda_i m_i - \lambda_j b &= \sum(\lambda_i m_i - \lambda_j b^i)\\ &= \sum(\lambda_i m_i - \lambda_j\varphi_j^i m_i) \in S.\end{aligned}$$

所以正如所要的，$x = \sum \lambda_i m_i + S = \lambda_j b + S$.

（ii）如果有某个 $t \ge i$ 使得 $\varphi_t^i m_i = 0$，则

$$\lambda_i m_i + S = \lambda_i m_i + (\lambda_t\varphi_t^i m_i - \lambda_i m_i) + S = S.$$

反之，如果 $\lambda_i m_i + S = 0$，则 $\lambda_i m_i \in S$，且有表达式

$$\lambda_i m_i = \sum_j a_j(\lambda_k\varphi_k^j m_j - \lambda_j m_j) \in S,$$

其中 $a_j \in R$. 我们要规格化这个表达式. 首先，对相关子引入下面的记号：如果 $j \le k$，定义

$$r(j,k,m_j) = \lambda_k\varphi_k^j m_j - \lambda_j m_j.$$

因 $a_j r(j,k,m_j) = r(j,k,a_j m_j)$，可以假定这个记号已经经过调正，从而使得

$$\lambda_i m_i = \sum_j r(j,k,m_j).$$

因 I 是有向集，可以选取一个指标 $t \in I$ 使它大于最后一个等式中出现的任一指标 i，j，k. 现在

$$\begin{aligned}\lambda_t\varphi_t^i m_i &= (\lambda_t\varphi_t^i m_i - \lambda_i m_i) + \lambda_i m_i\\ &= r(i,t,m_i) + \lambda_i m_i\\ &= r(i,t,m_i) + \sum_j r(j,k,m_j).\end{aligned}$$

其次，由正系统的定义，有 $\varphi_t^k\varphi_k^i = \varphi_t^i$，因而

$$\begin{aligned}r(j,k,m_j) &= \lambda_k\varphi_k^j m_j - \lambda_j m_j\\ &= (\lambda_t\varphi_t^j m_j - \lambda_j m_j) + [\lambda_t\varphi_t^k(-\varphi_k^j m_j) - \lambda_k(-\varphi_k^j m_j)]\\ &= r(j,t,m_j) + r(k,t,-\varphi_k^j m_j),\end{aligned}$$

508

因此，

$$\lambda_t\varphi_t^i m_i = \sum_\ell r(\ell,t,x_\ell),$$

其中 $x_\ell \in M_\ell$. 但对 $\ell \le t$ 容易验证

$$r(\ell,t,m_\ell) + r(\ell,t,m_\ell') = r(\ell,t,m_\ell + m_\ell').$$

所以可以把具有相同的较小指标 ℓ 的相关子合并起来，并记

$$\lambda_t\varphi_t^i m_i = \sum_\ell r(\ell,t,x_\ell)$$

$$= \sum_\ell \lambda_t \varphi_t^\ell x_\ell - \lambda_\ell x_\ell$$
$$= \lambda_t \left(\sum_\ell \varphi_t^\ell x_\ell\right) - \sum_\ell \lambda_\ell x_\ell,$$

其中 $x_\ell \in M_\ell$ 且所有指标 ℓ 是不同的．由直和中任一元素的表达式唯一可知，如果 $\ell \neq t$，则 $\lambda_\ell x_\ell = 0$，因 λ_ℓ 是内射，所以 $x_\ell = 0$. 因为 φ_t^t 是恒等映射，所以右端化简为 $\lambda_t \varphi_t^i m_t - \lambda_t m_t = 0$. 于是右端为 0，从而 $\lambda_t \varphi_t^i m_i = 0$. 因 λ_t 是内射，所以正如所要的 $\varphi_t^i m_i = 0$. ■

我们最初构造 $\varinjlim M_i$ 涉及 $\sum M_i$ 的商，即 $\varinjlim M_i$ 是一个余积的商．在集合范畴中，余积是不相交并 $\bigsqcup_i M_i$．我们可以把集合 X 的一个"商"看作 X 上某个等价关系的等价类的族．范畴的类似性暗示我们可以给出 $\varinjlim M_i$ 的第二种构造法，在 $\bigsqcup_i M_i$ 上使用等价关系．当指标集是有向集时，确实可以做到（见习题 7.65）．

例 7.99 （ⅰ）设 $\mathcal{I}$ 是模 A 的子模的全序族；即如果 $M, M' \in \mathcal{I}$，则不是 $M \subseteq M'$ 就是 $M' \subseteq M$. 则 $\mathcal{I}$ 是有向集，且 $\varinjlim M_i \cong \bigcup_i M_i$．

（ⅱ）如果 $\{M_i : i \in I\}$ 是模的某个族，则一切**有限部分和** $\mathcal{F}$ 是包含关系下的有向集，且 $\varinjlim M_i \cong \sum_i M_i$.

（ⅲ）如果 A 是模，则 A 的一切有限生成子模的族 $\mathrm{Fin}(A)$ 是有向集，且 $\varinjlim M_i \cong A$.

（ⅳ）如果 R 是整环和 $Q = \mathrm{Frac}(R)$，则一切形如 $\langle 1/r \rangle$ 的 Q 的循环 R-子模的族在包含关系下形成一个有向集，其中 $r \in R$ 和 $r \neq 0$，且 $\varinjlim M_i \cong Q$；即 Q 是循环模的正向极限． ■ 509

定义 设 $\{A_i, \alpha_j^i\}$ 和 $\{B_i, \beta_j^i\}$ 是同一指标集 I 上的正系统．一个**变换** $r: \{A_i, \alpha_j^i\} \to \{B_i, \beta_j^i\}$ 是指同态的一个加标族

$$r = \{r_i : A_i \to B_i\},$$

且对一切 $i \leq j$ 使得下图交换：

$$\begin{array}{ccc} A_i & \xrightarrow{r_i} & B_i \\ {\scriptstyle \alpha_j^i}\downarrow & & \downarrow{\scriptstyle \beta_j^i} \\ A_j & \xrightarrow[r_j]{} & B_j \end{array}$$

一个变换 $r: \{A_i, \alpha_j^i\} \to \{B_i, \beta_j^i\}$ 确定了一个同态

$$\vec{r} : \varinjlim A_i \to \varinjlim B_i,$$

它由

$$\vec{r} : \sum \lambda_i a_i + S \mapsto \sum \mu_i r_i a_i + T$$

给出，其中 $S \subseteq \sum A_i$，$T \subseteq \sum B_i$ 分别是构造 $\varinjlim A_i$ 和 $\varinjlim B_i$ 的关系子模，λ_i 和 μ_i 是 A_i 和 B_i 到直和中的内射．读者需验证：r 是正系统的变换蕴涵 $\vec{r}$ 不依赖于陪集代表元的选取，因此它是合理定义的函数．

命题 7.100 设 I 是有向集，并设 $\{A_i, \alpha_j^i\}$，$\{B_i, \beta_j^i\}$ 和 $\{C_i, \gamma_j^i\}$ 都是 I 上的正系统．如果 $r: \{A_i, \alpha_j^i\} \to \{B_i, \beta_j^i\}$ 和 $s: \{B_i, \beta_j^i\} \to \{C_i, \gamma_j^i\}$ 都是变换，且

$$0 \to A_i \xrightarrow{r_i} B_i \xrightarrow{s_i} C_i \to 0$$

对每个 $i \in I$ 都是正合列，则存在正合列

$$0 \to \varinjlim A_i \xrightarrow{\vec{r}} \varinjlim B_i \xrightarrow{\vec{s}} \varinjlim C_i \to 0.$$

注　*I 是有向集的假设只是为了证明 $\vec{r}$ 是单射.*

证明　我们只证明 $\vec{r}$ 是单射，因为剩下的正合性的证明是简单的. 假设 $\vec{r}(x)=0$，其中 $x\in \varinjlim A_i$. 因 I 是有向集，命题7.98(ⅰ)允许我们记 $x=\lambda_i a_i+S$（其中 $S\subseteq\sum A_i$ 是关系子模，λ_i 是 A_i 到直和中的内射）. 根据定义，$\vec{r}(x+S)=\mu_i r_i a_i+T$（其中 $T\subseteq\sum B_i$ 是关系子模，μ_i 是 B_i 到直和中的内射）. 现在命题7.98(ⅱ)证明在 $\varinjlim B_i$ 中 $\mu_i r_i a_i+T=0$ 蕴涵存在一个指标 $k\geq i$ 使得 $\beta_k^i r_i a_i=0$. 因 r 是正系统的变换，有

$$0=\beta_k^i r_i a_i=r_k\alpha_k^i a_i.$$

510　最后，因 r_k 是内射，有 $\alpha_k^i a_i=0$，因此 $x=\lambda_i a_i+S=0$，所以 $\vec{r}$ 是单射. ■

例 7.101　设 $\mathcal{U}$ 是 $\mathbb{R}$ 中包含 0 的一切开区间的族，用反包含定义偏序，并设 $\{B(U),\beta_V^U\}$ 是例 7.97(ⅵ)的正系统，其中

$$B(U)=\{f:U\to\mathbb{R}: f \text{ 是连续函数}\}$$

和 $\beta_V^U: f\mapsto f\mid V$.

现在我们提出 $\mathcal{U}$ 上的另外两个正系统. 定义点态乘法下的阿贝尔群

$$A(U)=\{\text{常数函数 } f:U\to\mathbb{Z}\}$$

和

$$C(U)=\{\text{连续函数 } f:U\to\mathbb{R}-\{0\}\},$$

则 $\{A(U),\alpha_V^U\}$ 和 $\{C(U),\gamma_V^U\}$ 都是正系统，其中 α 和 γ 都是限制映射.

这样定义变换 $s:\{B(U),\beta_V^U\}\to\{C(U),\gamma_V^U\}$，令 $s(U):B(U)\to C(U)$ 是映射 $f\mapsto e^{2\pi i f}$，并这样定义 $r:\{A(U),\alpha_V^U\}\to\{B(U),\beta_V^U\}$，令 $r(U):A(U)\to B(U)$ 是包含映射. 易知

$$0\to A(U)\xrightarrow{r_U} B(U)\xrightarrow{s_U} C(U)\to 0$$

对一切 U 都是正合列，从而命题 7.100 给出

$$0\to\varinjlim A(U)\to\varinjlim B(U)\to\varinjlim C(U)\to 0$$

的正合性. 容易验证 $\varinjlim A(U)\cong\mathbb{Z}$，因此 $\varinjlim B(U)\neq 0$. ■

有一个方法可以比较两个函子.

定义　*设 $F:\mathcal{C}\to\mathcal{D}$ 和 $G:\mathcal{C}\to\mathcal{D}$ 都是共变函子. 一个**自然变换**是指一族态射 $\tau=\{\tau_C: FC\to GC\}$，对 $\mathcal{C}$ 中每个对象 C 有一个态射，使得对 $\mathcal{C}$ 中的一切 $f:C\to C'$ 下图交换：*

$$\begin{array}{ccc} FC & \xrightarrow{Ff} & FC' \\ {\scriptstyle\tau_C}\downarrow & & \downarrow{\scriptstyle\tau_{C'}} \\ GC & \xrightarrow{Gf} & GC' \end{array}$$

*如果每个 τ_C 都是一个等价，则 τ 称为**自然等价**，称 F 和 G 是**自然等价的**.*

在反变函子之间也有类似定义的自然变换.

511　下一命题证明习题 7.5 中的同构 $\varphi_M:\mathrm{Hom}_R(R,M)\to M$ 构成一个自然变换.

命题 7.102　*如果 R 是交换环，则 $\mathrm{Hom}_R(R,M)$ 是一个 R-模，且由 $\varphi_M(f)=f(1)$ 给出的 R-同构*

$$\varphi_M : \mathrm{Hom}_R(R,M) \to M$$

组成一个自然等价 φ：$\mathrm{Hom}_R(R,\ )\to 1_R$，$1_R$ 是 **Mod** 上的单位函子．

注 命题 8.85 把这个命题推广到非交换环上的模．

证明 容易验证 φ_M 是可加函数．为证明 φ_M 是 R-同态，注意，因 f 是 R-映射，有

$$\varphi_M(rf) = (rf)(1) = f(1r) = f(r) = r[f(1)] = r\varphi_M(f),$$

考虑如下定义的函数 $M\to\mathrm{Hom}_R(R,M)$：如果 $m\in M$，则 $f_m : R\to M$ 由 $f_m(r)=rm$ 给出．易知 f_m 是一个 R-同态，且 $m\mapsto f_m$ 是 φ_M 的逆．

为证明同构 φ_M 构成自然等价，只要对任一模同态 $h : M\to N$ 证明下图交换：

$$\begin{array}{ccc} \mathrm{Hom}_R(R,M) & \xrightarrow{h_*} & \mathrm{Hom}_R(R,N) \\ \downarrow{\scriptstyle \varphi_M} & & \downarrow{\scriptstyle \varphi_N} \\ M & \xrightarrow{h} & N \end{array}$$

其中 $h_* : f\mapsto hf$. 设 $f : R\to M$. 沿顺时针方向走，$f\mapsto hf\mapsto hf(1)$，而反时针方向走，$f\mapsto f(1)\mapsto h(f(1))$. ■

对命题 7.92 证明的分析表明它可以如下进行推广：把 $\mathrm{Hom}(A,\ )$换成任意一个保持积的（共变）左正合函子 $F : {}_R\mathbf{Mod}\to\mathbf{Ab}$. 然而，这种推广只是一个错觉，因为 C. E. Watts 的一个定理给出这样的一个函子 F，存在模 A 使得 F 与 $\mathrm{Hom}_R(A,\ )$ 自然等价；即这些可表示的函子是被刻画好的．Watts 的另一个定理刻画了反变函子：如果 $G : {}_R\mathbf{Mod}\to\mathbf{Ab}$ 是反变左正合函子，它把和转变为积，则存在模 B 使得 G 和 $\mathrm{Hom}_R(\ ,B)$ 自然等价．Watts 定理的证明可以在 Rotman 所著的《An Introduction to Homological Algebra》77～79 页中找到．

例 7.103 （ⅰ）在命题 7.100 中，我们引入了从偏序指标集 I 上的一个正系统到另一个正系统的变换，如果回忆 I 上 R-模的一个正系统可以看作一个函子 $\mathbf{PO}(I)\to{}_R\mathbf{Mod}$，则读者可以看到这些变换都是自然变换． [512]

如果把偏序指标集上的逆系统看作反变函子，则也可以定义它们之间的变换（为自然变换）．

（ⅱ）选定一个点 p，令 $p=\{p\}$，我们断言 $\mathrm{Hom}(P,\ )$：集合范畴→集合范畴和集合范畴上的单位函子自然等价．如果 X 是一个集合，定义

$$\tau_X : \mathrm{Hom}(P,X) \to X \text{ 为 } f\mapsto f(p).$$

易知每个 τ_X 都是双射，我们现在证明 τ 是一个自然变换．设 X 和 Y 都是集合，并设 $h : X\to Y$，我们需要证明下图交换：

$$\begin{array}{ccc} \mathrm{Hom}(P,X) & \xrightarrow{h_*} & \mathrm{Hom}(P,Y) \\ \downarrow{\scriptstyle \tau_X} & & \downarrow{\scriptstyle \tau_Y} \\ X & \xrightarrow{h} & Y \end{array}$$

其中 $h_* : f\mapsto hf$. 顺时针方向走，$f\mapsto hf\mapsto hf(p)$，而反时针方向走，$f\mapsto f(p)\mapsto h(f(p))$.

（ⅲ）如果 k 是域，V 是域 k 上的向量空间，则它的对偶空间 V^* 是 V 上一切线性泛函的向量空间 $\mathrm{Hom}_k(V,k)$. 赋值映射 $e_v : f\mapsto f(v)$是 V^* 上的线性泛函，即 $e_v\in(V^*)^*=V^{**}$. 定义 $\tau_V : V\to V^{**}$ 为

$$\tau_V : v\mapsto e_v.$$

读者可以验证 τ 是从${}_k\mathbf{Mod}$ 上的单位函子到二重对偶函子的自然变换．τ 在一切有限维向量空间的子

范畴上的限制是自然等价. ■

环论中有一个有趣的部分发展了这个思想. 第一个问题是什么时候一个范畴$\mathcal{C}$“同构”于一个模范畴${}_R\mathbf{Mod}$. 关于这里的同构是什么意思我们有一点挑剔，它稍弱于这样的条件：存在函子 $F:\mathcal{C}\to{}_R\mathbf{Mod}$ 和 $G:{}_R\mathbf{Mod}\to\mathcal{C}$使得两个复合都等于单位函子.

定义 称函子 $F:\mathcal{C}\to\mathcal{D}$是一个**等价**，如果存在函子 $G:\mathcal{D}\to\mathcal{C}$使得复合 GF 和 FG 分别与单位函子 $1_\mathcal{C}$和 $1_\mathcal{D}$ 自然等价.

森田理论证明：如果 R 和 S 都是交换环，则它们的模范畴的等价蕴涵 $R\cong S$. 在第 9 章中，一旦引入了非交换环上的模，我们就会讲到一点森田理论，但读者真正要了解森田理论，应读 Jacobson 所著的《Basic Algebra II》或 Lam 所著的《Lectures on Modules and Rings》.

定义 给定函子 $F:\mathcal{C}\to\mathcal{D}$和 $G:\mathcal{D}\to\mathcal{C}$，则有序对$(F,G)$称为一个**伴随对**，如果对每对对象 $C\in\mathcal{C}$和 $D\in\mathcal{D}$，存在双射

513

$$\tau_{C,D}:\mathrm{Hom}_\mathcal{D}(FC,D)\to\mathrm{Hom}_\mathcal{C}(C,GD),$$

而且它们是 C 和 D 中的自然变换.

更详细地说，下面两个图交换：对$\mathcal{C}$中每个 $f:C'\to C$ 和$\mathcal{D}$中每个 $g:D\to D'$，

$$\begin{array}{ccc}\mathrm{Hom}_\mathcal{D}(FC,D) & \xrightarrow{(Ff)^*} & \mathrm{Hom}_\mathcal{D}(FC',D)\\ \downarrow{\tau_{C,D}} & & \downarrow{\tau_{C',D}}\\ \mathrm{Hom}_\mathcal{C}(C,GD) & \xrightarrow{f^*} & \mathrm{Hom}_\mathcal{C}(C',GD);\end{array}$$

$$\begin{array}{ccc}\mathrm{Hom}_\mathcal{D}(FC,D) & \xrightarrow{g_*} & \mathrm{Hom}_\mathcal{D}(FC,D')\\ \downarrow{\tau_{C,D}} & & \downarrow{\tau_{C,D'}}\\ \mathrm{Hom}_\mathcal{C}(C,GD) & \xrightarrow{(Gg)_*} & \mathrm{Hom}_\mathcal{C}(C,GD')\end{array}$$

这里是“伴随”这个词的词源. 设 $F=\oplus_R B:\mathbf{Mod}_R\to\mathbf{Mod}_S$，并设 $G=\mathrm{Hom}_S(B,\ ):\mathbf{Mod}_S\to\mathbf{Mod}_R$. 定理 8.99 中的同构是

$$\tau:\mathrm{Hom}_S(F(A),C)\to\mathrm{Hom}_R(A,G(C)).$$

如果把 Hom(,)当作一个内积，那么就使我们想起了线性代数中伴随对的定义：如果 $T:V\to W$ 是配置有内积的向量空间的线性变换，则它的伴随是线性变换 $T^*:W\to V$ 使得对一切 $v\in V$ 和一切 $w\in W$，

$$(Tv,w)=(v,T^*w).$$

例 7.104 (i) 设 U：群范畴→集合范畴是**底函子**，它把每个群 G 指派给它的底集，并把每个同态仅仅看作一个函数，又设 F：集合范畴→群范畴是**自由函子**，它把每个集合 X 指派给一个以 X 为基的自由群 FX. FX 是以 X 为基的自由群就是说，对每个群 H，每个函数 $\varphi:X\to H$ 对应唯一的同态 $\tilde{\varphi}:FX\to H$. 由此，如果 $\varphi:X\to Y$ 是任意函数，则 $\tilde{\varphi}:FX\to FY$；这就是 F 在态射上的定义：$F\varphi=\tilde{\varphi}$. 读者应明白函数 $f\mapsto f|X$ 是双射（它的逆是 $\varphi\mapsto\tilde{\varphi}$）

$$\tau_{X,H}:\mathrm{Hom}_{群范畴}(FX,H)\to\mathrm{Hom}_{集合范畴}(X,UH).$$

事实上，$\tau_{X,H}$是自然双射，表明(F,U)是函子的伴随对.

这个例子可以通过把群范畴换成其他有自由对象的范畴来加以推广，例如关于任意环 R 的${}_R\mathbf{Mod}$.

(ii) 伴随性是函子有序对的一个性质. 在 (i) 中，我们看到(F,U)是一个伴随对，其中 F 是自由函子，U 是底函子. 要是(U,F)也是伴随对，则有自然双射 $\mathrm{Hom}_{集合范畴}(UH,Y)\cong\mathrm{Hom}_{群范畴}(H,FY)$，

其中 H 是一个群，Y 是一个集合．这在一般情形下是不成立的，如果 H 是多于一个元素的有限群，Y 是多于一个元素的集合，则 $\mathrm{Hom}_{集合范畴}(UH,Y)$ 多于一个元素，而 $\mathrm{Hom}_{群范畴}(H,FY)$ 只有一个元素．所以 (U,F) 不是伴随对． [514]

（iii）下一章中我们将看到（定理 8.99），对每个共变 Hom 函子 $G=\mathrm{Hom}_R(A,\ )$，存在函子 F 使得 (F,G) 成为伴随对（$F=A\otimes_R$，叫做张量积）． ■

函子伴随对的更多的例子见 Mac Lane 所著的《Categories for the Working Mathematician》第 4 章，特别是 85～86 页．

设 (F,G) 是函子的伴随对，其中 $F:\mathcal{C}\to\mathcal{D}$ 和 $G:\mathcal{D}\to\mathcal{C}$．如果 $C\in\mathrm{obj}(\mathcal{C})$，则令 $D=FC$ 给出双射 $\tau:\mathrm{Hom}_{\mathcal{D}}(FC,FC)\to\mathrm{Hom}_{\mathcal{C}}(C,GFC)$，由此，定义 η_C 为

$$\eta_C=\tau(1_{FC}),$$

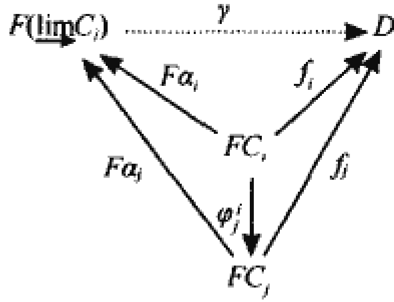
则 η_C 是态射 $C\to GFC$．习题 7.75 证明 $\eta:1_{\mathcal{C}}\to GF$ 是一个自然变换，它叫做伴随对的**单位**．

定理 7.105 设 (F,G) 是函子的伴随对，其中 $F:\mathcal{C}\to\mathcal{D}$ 和 $G:\mathcal{D}\to\mathcal{C}$，则 F 保持一切正向极限，G 保持一切反向极限．

注 （i）极限的指标集没有限制，特别是不必是有向集．

（ii）更精确的陈述是：如果 $\mathcal{C}$ 中存在 $\varinjlim C_i$，则 $\mathcal{D}$ 中存在 $\varinjlim FC_i$，且 $\varinjlim FC_i\cong F(\varinjlim C_i)$．

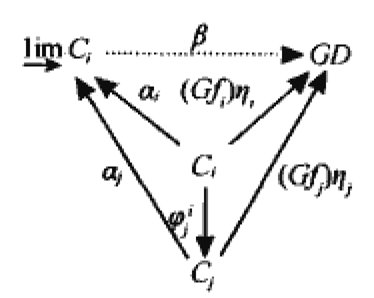
证明 设 I 是偏序集，并设 $\{C_i,\varphi_j^i\}$ 是 $\mathcal{C}$ 中 I 上的正系统．易知 $\{FC_i,F\varphi_j^i\}$ 是 $\mathcal{D}$ 中 I 上的正系统．考虑 $\mathcal{D}$ 中下面的图：



其中 $\alpha_i:C_i\to\varinjlim C_i$ 是正向极限定义中的映射．我们需要证明存在唯一的态射 $\gamma:F(\varinjlim C_i)\to D$ 使得这个图交换．我们的想法是把 G 作用到这个图上，并用单位 $\eta:1_X\to GF$ 分别把 $GF(\varinjlim C_i)$ 和 GFC_i 替换为 $\varinjlim C_i$ 和 C_i．更详细地说，根据习题 7.75，存在态射 η 和 η_i 使得下图交换： [515]

$$\begin{array}{ccc}\varinjlim C_i & \xrightarrow{\eta} & GF(\varinjlim C_i)\\ \uparrow{\scriptstyle\alpha_i} & & \uparrow{\scriptstyle GF\alpha_i}\\ C_i & \xrightarrow{\eta_i} & GFC_i\end{array}$$

把它和 G 作用后的原始图组合起来给出下图的交换性：



根据正向极限的定义，存在唯一的 $\beta:\varinjlim C_i\to GD$ 使得图交换，即 $\beta\in\mathrm{Hom}_{\mathcal{C}}(\varinjlim(C_i,GD))$．因 (F,G) 是伴随对，存在自然双射

$$\tau:\mathrm{Hom}_{\mathcal{D}}(F(\varinjlim C_i),D)\to\mathrm{Hom}_{\mathcal{C}}(\varinjlim C_i,GD).$$

定义

$$\gamma = \tau^{-1}(\beta) \in \mathrm{Hom}_{\mathcal{D}}(F(\varinjlim C_i), D).$$

我们断言 $\gamma: F(\varinjlim C_i) \to D$ 使得第一个图交换．伴随性定义中第一个交换正方形给出下图的交换性：

$$\begin{array}{ccc}
\mathrm{Hom}_{\mathcal{C}}(\varinjlim C_i, GD) & \xrightarrow{\alpha_i^*} & \mathrm{Hom}_{\mathcal{C}}(C_i, GD) \\
\downarrow \tau^{-1} & & \downarrow \tau^{-1} \\
\mathrm{Hom}_{\mathcal{D}}(F(\varinjlim C_i), D) & \xrightarrow{(F\alpha_i)^*} & \mathrm{Hom}_{\mathcal{D}}(FC_i, D)
\end{array}$$

因此，$\tau^{-1}\alpha_i^* = (F\alpha_i)^*\tau^{-1}$. 两个函数都在 β 上赋值，有

$$(F\alpha_i)^*\tau^{-1}(\beta) = (F\alpha_i)^*\gamma = \gamma F\alpha_i.$$

另一方面，因 $\beta\alpha_i = (Gf_i)\eta_i$，有

516

$$\tau^{-1}\alpha_i^*(\beta) = \tau^{-1}(\beta\alpha_i) = \tau^{-1}((Gf_i)\eta_i).$$

所以

$$\gamma F\alpha_i = \tau^{-1}((Gf_i)\eta_i).$$

伴随性定义中的第二个交换正方形给出下图的交换性：

$$\begin{array}{ccc}
\mathrm{Hom}_{\mathcal{D}}(FC_i, FC_i) & \xrightarrow{(f_i)_*} & \mathrm{Hom}_{\mathcal{D}}(FC_i, D) \\
\downarrow \tau & & \downarrow \tau \\
\mathrm{Hom}_{\mathcal{C}}(C_i, GFC_i) & \xrightarrow{(Gf_i)_*} & \mathrm{Hom}_{\mathcal{C}}(C_i, GD)
\end{array}$$

即

$$\tau(f_i)_* = (Gf_i)_*\tau.$$

在 1_{FC_i} 处赋值，η_i 的定义给出 $\tau(f_i)_*(1) = (Gf_i)_*\tau(1)$，从而 $\tau f_i = (Gf_i)_*\eta_i$. 所以，

$$\gamma F\alpha_i = \tau^{-1}((Gf_i)\eta_i) = \tau^{-1}\tau f_i = f_i,$$

因此，γ 使得原始图交换．

我们把 γ 唯一性的证明留给读者作为练习，提示用 β 的唯一性．

对偶的证明表明 G 保持反向极限． ■

关于函子成为伴随对的一员有一个充分必要条件，叫做**伴随函子定理**，见 Mac Lane 所著的《Categories for the Working Mathematician》117 页．

习题

7.65 设 $\{M_i, \varphi_j^i\}$ 是 R-模的正系统，I 是指标集，并设 $\bigsqcup_i M_i$ 是不相交并．在 $\bigsqcup_i M_i$ 上定义 $m_i \sim m_j$，其中 $m_i \in M_i$ 和 $m_j \in M_j$，如果存在满足 $k \geq i$ 和 $k \geq j$ 的指标 k 使得 $\varphi_k^i m_i = \varphi_k^j m_j$.

(i) 证明 $\sim$ 是 $\bigsqcup_i M_i$ 上的等价关系．

(ii) 记 m_i 的等价类为 $[m_i]$，并用 L 表示一切这种等价类的族．证明下面的定义给 L 以 R-模结构：

$$\text{如果 } r \in R, r[m_i] = [rm_i];$$

$$[m_i] + [m_j'] = [\varphi_k^i m_i + \varphi_k^j m_j'], \text{其中 } k \geq i \text{ 和 } k \geq j.$$

(iii) 证明 $L \cong \varinjlim M_i$.

提示：用命题 7.98.

7.66 设 $\{M_i, \varphi_j^i\}$ 是 R-模的正系统，并设 $F: {}_R\mathbf{Mod} \to \mathcal{C}$ 是到某个范畴 $\mathcal{C}$ 的函子．证明：当 F 是共变函子时，

$\{FM_i, F\varphi_j^i\}$ 是$\mathcal{C}$中的正系统，而当 F 是反变函子时，$\{FM_i, F\varphi_j^i\}$ 是$\mathcal{C}$中的逆系统．

517

7.67 举出某个有向指标集 I 上一个模的正系统的例子 $\{A_i, \alpha_j^i\}$，其中对一切 i，$A_i \neq \{0\}$，而 $\varinjlim A_i = \{0\}$．

7.68 （i）设 K 是有向指标集 I 的共尾子集（即对每个 $i \in I$，存在 $k \in K$ 使得 $i \leq k$），设 $\{M_i, \varphi_j^i\}$ 是 I 上的正系统，又设 $\{M_i, \varphi_j^i\}$ 是指标在 K 中的子正系统．证明 I 上的正向极限同构于 K 上的正向极限．

（ii）一个偏序集 I 有**顶元素**，如果存在 $\infty \in I$ 使得对一切 $i \in I$ 有 $i \leq \infty$．如果 $\{M_i, \varphi_j^i\}$ 是 I 上的正系统，证明

$$\varinjlim M_i \cong M_\infty.$$

（iii）证明：如果指标集不是有向集，则（i）可能不成立．

提示：推出．

7.69 设$\mathcal{C}$和$\mathcal{D}$都是范畴，并用 $\mathcal{F}(\mathcal{C},\mathcal{D})$ 表示一切（共变）函子$\mathcal{C}\to\mathcal{D}$的类．如果定义

$$\mathrm{Hom}(F,G) = \{\text{一切自然变换 } F \to G\},$$

证明$\mathcal{F}(\mathcal{C},\mathcal{D})$是范畴．

注：有一个集合论的技术问题，即为什么 $\mathrm{Hom}(F,G)$是一个集合（而不是本性类）？答案是它有可能不是集合，解决这个问题的最容易的方法（但不是唯一的）是假定$\mathcal{C}$和$\mathcal{D}$中的对象形成集合，即$\mathcal{C}$和$\mathcal{D}$都是小范畴．这里我们允许读者这样做．

7.70 称函子 $T: {}_R\mathbf{Mod}\to\mathbf{Ab}$ 为**可表示的**，如果存在 R-模 A 和自然等价 $\tau: T\to \mathrm{Hom}_R(A, \ )$．证明：如果 $\mathrm{Hom}_R(A, \ )$和 $\mathrm{Hom}_R(B, \ )$都是自然等价，则 $A\cong B$．由此推出，如果一个可表示的函子 T 自然等价于 $\mathrm{Hom}_R(A, \ )$，如不计同构，则 A 被 T 确定．

7.71 如果${}_k\mathbf{V}$是域 k 上一切有限维向量空间的范畴，证明二重对偶 $V\mapsto V^{**}$ 自然等价于单位函子．

7.72 设$\{E_i, \varphi_j^i\}$是有向指标集 I 上内射 R-模的正系统．证明：如果 R 是诺特环，则 $\varinjlim E_i$ 是内射模．

提示：用命题 7.69.

7.73 考虑 $k[x]$中的理想 $I=(x)$，其中 k 是交换环．证明多项式环 $k[x]$的完备化是 $k[[x]]$，即形式幂级数环．

7.74 设 $r: \{A_i, \alpha_j^i\}\to\{B_i, \beta_j^i\}$和 $s: \{B_i, \beta_j^i\}\to\{C_i, \gamma_j^i\}$是指标集 I 上逆系统的变换．如果对每个 $i\in I$，

$$0 \to A_i \xrightarrow{r_i} B_i \xrightarrow{s_i} C_i$$

是正合列，证明存在正合列

$$0 \to \varprojlim A_i \xrightarrow{\vec{r}} \varprojlim B_i \xrightarrow{\vec{s}} \varprojlim C_i.$$

7.75 设(F,G)是函子的伴随对，其中 $F: \mathcal{C}\to\mathcal{D}$和 $G: \mathcal{D}\to\mathcal{C}$，并设 $\tau_{C,D}: \mathrm{Hom}(FC,D)\to\mathrm{Hom}(C,GC)$是自然双射．

（i）如果 $D=FC$，则有自然双射

$$\tau_{C,FC}: \mathrm{Hom}(FC,FC) \to \mathrm{Hom}(C,GFC)$$

且 $\tau(1_{FC})=\eta_C\in\mathrm{Hom}(C,GFC)$．证明$\eta$：$1_{\mathcal{C}}\to GF$ 是自然变换．

518

（ii）如果 $C=GD$，则有自然双射

$$\tau_{GD,D}^{-1}: \mathrm{Hom}(GD,GD) \to \mathrm{Hom}(FGD,D)$$

且 $\tau^{-1}(1_D)=\varepsilon_D\in\mathrm{Hom}(FGD,D)$．证明 $\varepsilon: FG\to 1_{\mathcal{D}}$是自然变换（我们称 ε 为伴随对的**余单位**．）

7.76 如果 I 是偏序集，$\mathcal{C}$是范畴，则 I 上$\mathcal{C}$的**预层**是指反变函子$\mathcal{F}: \mathbf{PO}(I)\to\mathcal{C}$．

（i）如果 I 是$\mathbb{R}$中包含 0 的一切开区间 U 的族，证明例7.97(vi)中的$\mathcal{F}$是一个阿贝尔群的预层．

（ii）设 X 是拓扑空间，并设 I 是元素为 X 中开集的偏序集．定义 I 上到 $\mathbf{Ab}$ 的预层序列$\mathcal{F}'\to\mathcal{F}\to\mathcal{F}''$是**正合的**，如果对每个 $U\in I$，

$$\mathcal{F}'(U) \to \mathcal{F}(U) \to \mathcal{F}''(U)$$

是正合列．如果$\mathcal{F}$是 I 上的预层，定义$\mathcal{F}$在 $x \in X$ 处的茎$\mathcal{F}_x$ 为

$$\mathcal{F}_x = \varinjlim_{U \ni x} \mathcal{F}(U).$$

如果$\mathcal{F}' \to \mathcal{F} \to \mathcal{F}''$是预层的正合列，证明对每个 $x \in X$ 存在茎的正合列

$$\mathcal{F}'_x \to \mathcal{F}_x \to \mathcal{F}''_x.$$

7.77 (i) 设 F：群范畴→**Ab** 是 $F(G)=G/G'$的函子，其中 G'是群 G 的换位子群，并设 U：**Ab**→群范畴是把每个阿贝尔群 A 映入它自己的函子（即 UA 不必把 A 看作阿贝尔群）．证明(F,U)是函子的伴随对．

(ii) 证明伴随对(F,U)的单位是自然映射 $G \to G/G'$.

7.78 证明：如果 T：${}_R$**Mod**→**Ab** 是保持积的加性左正合函子，则 T 保持反向极限．

7.79 推广命题 5.4 为允许有无限个直和项．设$\{S_i : i \in I\}$是一个 R-模 M 的子模的族，其中 R 是交换环．如果 $M=\langle \bigcup_{i \in I} S_i \rangle$，则下列条件等价．

(i) $M=\sum_{i \in I} S_i$.

(ii) 每个 $a \in M$ 有形如$a = s_{i_1} + \cdots + s_{i_n}$ 的唯一表达式，其中 $s_{i_j} \in S_{i_j}$.

(iii) 对每个 $i \in I$，

519

$$S_i \cap \langle \bigcup_{j \neq i} S_j \rangle = \{0\}.$$

第8章　代　　数

本章介绍非交换环和非交换环上的模．我们先证明模就是用另一种方式来看待环的表示，即环元素可以看作阿贝尔群上的算子．随后证明韦德伯恩-阿廷定理，它给出了半单环的分类，以及Maschke定理，它说群代数通常都是半单的．在研究张量积，即一种和Hom函子密切相关的结构（由于伴随同构）的间隔之后，我们引入有限群的表示和特征标，这个讨论随即用来证明伯恩赛德和弗罗贝尼乌斯的群论定理．

8.1　非交换环

到现在为止我们考虑的环都是交换环，但还有非交换环的重要例子．

定义　*环 R 是指一个加性阿贝尔群，它配置一个乘法 $R\times R\to R$ 并记为 $(a,b)\mapsto ab$，对一切 $a,b,c\in R$ 满足*

（i）$a(bc)=(ab)c$；

（ii）$a(b+c)=ab+ac$ 和 $(b+c)a=ba+ca$；

（iii）*存在 $1\in R$ 使得对一切 $a\in R$，*

$$1a=a=a1.$$

下面是环的一些例子，它们是不交换的．

例8.1　（i）如果 k 是任意交换环，则元素在 k 中的一切 $n\times n$ 矩阵 $\mathrm{Mat}_n(k)$ 是在矩阵加法和矩阵乘法下的环，它是交换的当且仅当 $n=1$.

520

如果 k 不交换，$\mathrm{Mat}_n(k)$ 也是环，这是因为通常矩阵乘法的定义仍然有意义：如果 $A=[a_{ij}]$ 和 $B=[b_{ij}]$ 则 AB 的 ij 元素是 $\sum_p a_{ip}b_{pj}$，正好保证 A 中的元素恒出现在左方，而 B 的元素恒出现在右方．

（ii）如果 k 是任意交换环，G 是群（它的运算写作乘法），则我们定义**群代数** kG 如下：它的加法阿贝尔群是自由 k-模，这个模的基以 G 的元素加标；这样，每个元素有形如 $\sum_{g\in G}a_g g$ 的唯一的表达式，其中对一切 $g\in G, a_g\in k$ 且几乎一切 $a_g=0$，即只有有限个非零的 a_g. 如果 g 和 h 都是基元素（即 g，$h\in G$），定义它们在 kG 中的积为它们在 G 中的积 gh，而只要 $a\in k$ 和 $g\in G$ 就有 $ag=ga$. kG 中任意两个元素的积由线性扩张定义：

$$\Big(\sum_{g\in G}a_g g\Big)\Big(\sum_{h\in G}b_h h\Big)=\sum_{z\in G}\Big(\sum_{gh=z}a_g b_h\Big)z.$$

一个群代数 kG 是交换的当且仅当群 G 是阿贝尔群．

在习题8.17中，我们给出 kG 的另一种描述，当 G 是有限群时，可以作为在点态加法和卷积下的一切函数 $G\to k$.

（iii）一个阿贝尔群 A 的**自同态**是指同态 $f:A\mapsto A$. A 的**自同态环**记为 $\mathrm{End}(A)$，是指一切自同态的集合，它的加法是点态加法

$$f+g:a\mapsto f(a)+g(a),$$

它的乘法是复合．容易验证 $\mathrm{End}(A)$ 总是环，并有简单的例子表明它是不交换的．例如 p 是素数，

则 $\mathrm{End}(\mathbb{I}_p \oplus \mathbb{I}_p) \cong \mathrm{Mat}_2(\mathbb{F}_p)$.

(iv) 设 k 是环，并设 $\sigma: k \to k$ 是环自同态．在 $k[x] = \left\{ \sum_i a_i x^i : a_i \in k \right\}$ 上定义一个新的乘法为

$$xa = \sigma(a)x.$$

于是，两个多项式的乘法由下式给出，

$$\left(\sum_i a_i x^i\right)\left(\sum_j b_j x^j\right) = \sum_r c_r x^r,$$

其中 $c_r = \sum_{i+j=r} a_i \sigma^i(b_j)$．容易验证配置了这个新的乘法的 $k[x]$ 未必是交换环．我们记这个环为 $k[x;\sigma]$，把它叫做**斜多项式环**．

(v) 如果 $R_1, \cdots, R_t$ 是环，则它们的**直积**

$$R = R_1 \times \cdots \times R_t$$

是指具有坐标状态的加法和乘法的笛卡儿积：

$$(r_i) + (r_i') = (r_i + r_i'), (r_i)(r_i') = (r_i r_i');$$

521 我们把 $(r_1, \cdots, r_t)$ 缩写为 (r_i).

易知 $R = R_1 \times \cdots \times R_t$ 是环．我们把 $r_i \in R_i$ 等同于第 i 个坐标是 r_i 而其他坐标都是 0 的"向量"．如果 $i \neq j$，则 $r_i r_j = 0$．

(vi) **除环** D（或**体**）是指一个"非交换域"，即 D 是一个环，其中 $1 \neq 0$ 且每个非零元素 $a \in D$ 有乘法逆：存在 $a' \in D$ 使得 $aa' = 1 = a'a$．等价地说，环 D 是除环，如果它的非零元素的集合 $D^\times$ 形成乘法下的群．当然，域是除环，下面是一个非交换的例子．

设 $\mathbb{H}$ 是 $\mathbb{R}$ 上的四维向量空间，标记一个基为 $1, i, j, k$．于是 $\mathbb{H}$ 中的一个典型元素 h 是

$$h = a + bi + cj + dk,$$

其中 $a, b, c, d \in \mathbb{R}$．我们定义基元素的乘法如下：

$$i^2 = j^2 = k^2 = -1;$$

$$ij = k = -ji; \quad jk = i = -kj; \quad ki = j = -ik,$$

我们强调每个元素 $a \in \mathbb{R}$ 与 $1, i, j, k$ 可交换．如果现在用线性扩张定义任意元素的乘法，则 $\mathbb{H}$ 是环，叫做（实）**四元数**[⊖]（乘法的结合性来自四元数群 $\mathbf{Q} = \{\pm 1, \pm i, \pm j, \pm k\}$ 中乘法的结合性）．为证明 $\mathbb{H}$ 是除环，只要求出非零元素的逆．定义 $u = a + bi + cj + dk \in \mathbb{H}$ 的**共轭**为

$$\overline{u} = a - bi - cj - dk;$$

易知

$$u\overline{u} = a^2 + b^2 + c^2 + d^2.$$

因此，当 $u \neq 0$ 时，$u\overline{u} \neq 0$，从而

$$u^{-1} = \overline{u}/u\overline{u} = \overline{u}(a^2 + b^2 + c^2 + d^2).$$

不难证明共轭是加性同构且满足

$$\overline{uw} = \overline{w}\,\overline{u}.$$

正如高斯整数用来证明费马二平方和定理（定理 3.66）——一个奇素数 p 是两个平方数的和当且

⊖ 四元数由哈密顿（W. R. Hamilton）在 1843 年发现，当时他要寻找复数的一种推广，从而把它应用到某种物理现象的模型上．为此他希望构造出一个三维代数，但是只有当他看到三维应该用四维代替时他才能成功．这就是为什么哈密顿把 $\mathbb{H}$ 叫做四元数，为纪念哈密顿把这个除环记为 $\mathbb{H}$．

仅当$p\equiv 1\bmod 4$——四元数也可以用来证明拉格朗日定理：每个正整数都是四个平方数的和（见Samuel所著的《Algebraic Theory of Numbers》，82～85页）．

在构造H时，只用到域R这样的性质：非零数的平方和非零，R的任一子域也有这个性质，但C没有．例如，存在有理四元数的除环．

在第10章中讨论叉积代数时，我们将构造其他除环的例子．■ [522]

注 某些数学家在环的定义中不假定必须包含幺元1．他们举出一些很自然的例子，如偶整数或可积函数，一个函数$f:[0,\infty)\to\mathbb{R}$是可积的，如果

$$\int_0^\infty |f(x)|\,\mathrm{d}x=\lim_{t\to\infty}\int_0^t |f(x)|\,\mathrm{d}x<\infty.$$

不难看出，如果f和g可积，则它们的点态和$f+g$与点态积fg也是可积的．幺元的唯一候选者是常数函数e，即对一切$x\in[0,\infty),e(x)=1$，但显然e是不可积的．

然而幺元的缺席使得许多构造更加复杂．例如，如果R是"没有幺元的环"，$a\in R$，则把a生成的主理想(a)定义为$(a)=\{ra:r\in R\}$将导致$a\notin(a)$的可能性，由此，我们必须重新定义(a)以迫使a在里面．多项式环变得很奇怪：如果R没有幺元，则$x\notin R[x]$．还有其他（更重要的）理由需要幺元，但这些例子足以表明不假定有幺元会导致某种不方便，所以我们决定强调环要有幺元．

习题8.1 证明每个"无幺元的环"可以作为一个理想嵌入一个（有幺元的）环．

环R的子环S是包含在R中的一个环，满足$1\in S$，且对$s,s'\in S$，它们的和$s+s'$和积ss'在S中和在R中有相同的意义．下面是正式定义．

定义 环R的**子环**S是指R的子集满足

（i）$1\in S$；

（ii）如果$a,b\in S$，则$a-b\in S$；

（iii）如果$a,b\in S$，则$ab\in S$．

例8.2 （i）环R的**中心**（记为$Z(R)$）是指和每个元素都可交换的一切元素$z\in R$的集合：

$$Z(R)=\{z\in R:\text{对一切}\ r\in R,zr=rz\}.$$

易知$Z(R)$是R的子环．如果k是交换环，则$k\subseteq Z(kG)$．习题8.10要求证明矩阵环的中心$Z(\mathrm{Mat}_n(R))$是一切**标量矩阵**aI的集合，其中$a\in Z(R)$，I是单位矩阵，习题8.11说$Z(\mathbb{H})=\{a1:a\in\mathbb{R}\}$．

（ii）如果D是除环，则它的中心$Z(D)$是域．此外，如果$D^\times$是D的非零元素的乘法群，则$Z(D^\times)=Z(D)^\times$，即乘法群$D^\times$的中心由$Z(D)$的非零元素组成．■

下面是两个不是子环的例子． [523]

例8.3 （i）定义$S=\{a+ib:a,b\in\mathbb{Z}\}\subseteq\mathbb{C}$．定义$S$中的加法为C中的加法，而定义$S$中的乘法为

$$(a+bi)(c+di)=ac+(ad+bc)i$$

（于是，在S中$i^2=0$，而在C中$i^2\neq 0$）．容易验证S是环，但它不是C的子环．

（ii）如果$R=\mathbb{Z}\times\mathbb{Z}$，则它的幺元是（1，1）．设

$$S=\{(n,0)\in\mathbb{Z}\times\mathbb{Z}:n\in\mathbb{Z}\}.$$

容易验证S在加法和乘法下封闭，因为$(1,0)$是S中的幺元，所以S的确是环．然而S不包含R的幺元，所以S不是R的子环．■

非交换性立即产生的一种复杂化是理想的概念被分裂为三个概念，现在有左理想、右理想和双边理想．

定义 设 R 是环，并设 I 是 R 的加法子群．则 I 称为**左理想**，如果 $a \in I$ 和 $r \in R$ 蕴涵 $ra \in I$，而 I 称为**右理想**，如果 $ar \in I$．如果 I 既是左理想又是右理想，则称 I 为**双边理想**．

例 8.4 在 $\mathrm{Mat}_2(\mathbb{R})$ 中，等式

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} u & 0 \\ v & 0 \end{bmatrix} = \begin{bmatrix} * & 0 \\ * & 0 \end{bmatrix}$$

表明“第一列”（即除第一列外都是 0 的矩阵）形成一个左理想（“第二列”也形成一个左理想）．等式

$$\begin{bmatrix} u & v \\ 0 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} * & * \\ 0 & 0 \end{bmatrix}$$

表明“第一行”（即除第一行外都是 0 的矩阵）形成一个右理想（“第二行”也形成一个右理想）．读者可以验证这些单边理想没有一个是双边理想．其实，双边理想只有 $\{0\}$ 和 $\mathrm{Mat}_2(\mathbb{R})$ 自己．这个例子可以用一种明显的方式加以推广，从而对每个环 k 和一切 $n \geqslant 2$ 给出 $\mathrm{Mat}_n(k)$ 中左理想和右理想的例子． ■

例 8.5 在环的直积 $R = R_1 \times \cdots \times R_t$ 中，每个 R_j 等同于

$$R_j = \{(0,\cdots,0,r_j,0,\cdots,0) : r_j \in R_j\},$$

其中 r_j 出现在第 j 个坐标中．易知每个 R_j 都是 R 中的一个双边理想（因为如果 $j \neq i$，则 $r_j r_i = 0$ 和 $r_i r_j = 0$）．此外，R_j 中的任一左理想或右理想也是 R 中的左理想或右理想． ■

524

环同态 $\varphi: R \to S$ 的定义恰如交换的情形，我们将看到它们的核是双边理想．下一节定义的零化子理想是双边理想的另一个来源．

定义 如果 R 和 S 是环，则**环同态**（或环映射）是指函数 $\varphi: R \to S$，对一切 $r, r' \in R$ 满足

（i）$\varphi(r + r') = \varphi(r) + \varphi(r')$；

（ii）$\varphi(rr') = \varphi(r)\varphi(r')$；

（iii）$\varphi(1) = 1$.

如果 $\varphi: R \to S$ 是环同态，则**核**的定义和通常一样：

$$\ker\varphi = \{r \in R : \varphi(r) = 0\}.$$

象的定义也和通常一样：

$$\mathrm{im}\varphi = \{s \in S : s \text{ 有某个 } r \in R \text{ 使得 } s = \varphi(r)\}.$$

核恒为双边理想，因为如果 $\varphi(a) = 0$ 和 $r \in R$，则

$$\varphi(ra) = \varphi(r)\varphi(a) = 0 = \varphi(a)\varphi(r) = \varphi(ar),$$

从而 $a \in \ker\varphi$ 蕴涵 ra 和 ar 都在 $\ker\varphi$ 中．另一方面，$\mathrm{im}\varphi$ 只是 S 的子环．

当 I 是双边理想时，我们可以形成**商环** R/I，因为由 $(r+I)(s+I) = rs + I$ 给出的阿贝尔商群 R/I 上的乘法是合理定义的：如果 $r + I = r' + I$ 和 $s + I = s' + I$，则 $rs + I = r's' + I$．即如果 $r - r' \in I$ 和 $s - s' \in I$，则 $rs - r's' \in I$．要证明这一点，注意

$$rs - r's' = rs - rs' + rs' - r's' = r(s - s') + (r - r')s \in I,$$

这是因为 $s - s'$ 和 $r - r'$ 都在 I 中，而 I 是双边理想，所以右边的每个项都在 I 中．易知由 $r \mapsto r + I$

（和通常一样）定义的**自然映射** $\pi: R \to R/I$ 是环映射．容易验证同构定理和对应定理对（非交换）环成立．

当 R 是不必交换的任意环时，我们定义 R-模．对照交换的情形，现在有两种不同的 R-模：左 R-模和右 R-模．**左R-模**我们已经定义了（虽然到现在为止我们一直叫它 R-模）．

定义　设 R 是环．一个**左** R-**模**是指一个（加法）阿贝尔群 M，配置以**标量乘法** $R \times M \to M$，记为

$$(r,m) \mapsto rm,$$

使得对一切 $m,m' \in M$ 和一切 $r,r',1 \in R$，下列公理成立：

525

（i）$r(m+m') = rm + rm'$；

（ii）$(r+r')m = rm + r'm$；

（iii）$(rr')m = r(r'm)$；

（iv）$1m = m$.

定义　一个**右** R-**模**是指一个（加法）阿贝尔群 M，配置以**标量乘法** $M \times R \to M$，记为

$$(m,r) \mapsto mr,$$

使得对一切 $m,m' \in M$ 和一切 $r,r',1 \in R$ 下列公理成立：

（i）$(m+m')r = mr + m'r$；

（ii）$m(r+r') = mr + mr'$；

（iii）$m(rr') = (mr)r'$；

（iv）$m1 = m$.

记号　记左 R-模 M 为 ${}_RM$，记右 R-模 M 为 M_R.

当然，把右 R-模中的标量乘法记为 $(m,r) \mapsto rm$ 也没有什么妨碍，如果这样做，则我们看到只有公理（iii）和左 R-模的公理不同，右边的版本现在要读作

$$(rr')m = r'(rm).$$

这两个定义的真正差别是由理想产生的．环 R 中的左理想是左 R-模，右理想是右 R-模，在例 8.4 中我们看到它们是不同的东西．

子模的定义是明显的，它是在标量乘法下封闭的子群．注意环 R 可以看作一个左 R-模（记为${}_RR$）或一个右 R-模（记为 R_R）．${}_RR$ 的子模是左理想，R_R 的子模是右理想．如果 N 是左 R-模 M 的子模，则**商模**M/N 是通过定义标量乘法为 $r(m+N) = rm + N$，以做成一个左 R-模的商群．

定义　称右 R-模 M 和 N 之间的一个加性函数 $f: M_R \to N_R$ 为 R-**同态**（或 R-映射），如果对一切 $m \in M$ 和 $r \in R$，$f(mr) = f(m)r$．一切右 R-模和 R-映射构成一个范畴，记为 $\mathbf{Mod}_R$．记号 ${}_R\mathbf{Mod}$ 已经引入用来表示一切左 R-模的范畴．在这两个范畴中我们都用

$$\mathrm{Hom}_R(M,N)$$

来表示 R-模 M 和 N 之间的一切 R-映射的集合，其中 M 和 N 是同一边的 R-模．

526

例 8.6　设 G 是群，k 是交换环，并设 A 是左 kG-模．定义 G 在 A 上的一个新的作用（记为 $g*a$）为

$$g*a = g^{-1}a,$$

其中 $a \in A$ 和 $g \in G$. 对 kG 的任意元素，定义

$$\Big(\sum_{g \in G} m_g g\Big) * a = \sum_{g \in G} m_g g^{-1} a.$$

易知在这个新的作用下，A 是一个右 kG-模；即如果 $u \in kG$ 和 $a \in A$，由$(a,u) \mapsto u*a$ 给出的函数

$A\times kG\to A$满足右模定义中的公理．当然，我们通常把 $u*a$ 写作au. 于是，一个 kG-模既可以看作左也可以看作右 kG-模． ■

例 8.7 我们现在推广例 8.1(iii). 如果 M是左 R-模，则称 R-映射 $f:M\to M$为 M的 **R-自同态**. M的一切 R-自同态的集合叫做**自同态环**，记为 $\mathrm{End}_R(M)$. 作为集合，$\mathrm{End}_R(M)=\mathrm{Hom}_R(M,M)$，我们已经看到它是一个加法阿贝尔群．现在定义乘法为复合：如果 $f,g:M\to M$，则 $fg:m\mapsto f(g(m))$.

如果把 M 看作一个阿贝尔群，则记例 8.1（iii）中定义的自同态环 $\mathrm{End}(M)$（没有下标）为 $\mathrm{End}_{\mathbb{Z}}(M)$，$\mathrm{End}_R(M)$ 是 $\mathrm{End}_{\mathbb{Z}}(M)$ 的子环． ■

我们现在要证明环元素可以看作一个阿贝尔群上的算子（即自同态）．

定义 环 R 的一个**表示**是指环同态

$$\sigma: R\to \mathrm{End}_{\mathbb{Z}}(M),$$

其中 M 是一个阿贝尔群．

环的表示可以翻译为模的语言．

命题 8.8 每个表示 $\sigma:R\to\mathrm{End}_{\mathbb{Z}}(M)$ 把 M 配置成一个左 R-模结构，其中 M 是阿贝尔群．反之，每个左 R-模确定一个表示 $\sigma:R\to\mathrm{End}_{\mathbb{Z}}(M)$．

证明 给定一个同态 $\sigma:R\to\mathrm{End}_{\mathbb{Z}}(M)$，记 $\sigma(r):M\to M$为 σ_r，并定义标量乘法 $R\times M\to M$为

527

$$rm=\sigma_r(m),$$

其中 $m\in M$. 经简单计算可知配置以这个标量乘法的 M 是一个左 R-模．

反之，假定 M 是一个左 R-模．如果 $r\in R$，则 $m\mapsto rm$ 定义了一个自同态 $T_r:M\to M$. 容易验证由 $\sigma:r\to T_r$ 给出的函数 $\sigma:R\to\mathrm{End}_{\mathbb{Z}}(M)$ 是一个表示． ■

定义 称一个左 R-模为**忠实的**，如果对一切 $r\in R$，只要对一切 $m\in M$ 有 $rm=0$，则 $r=0$.

当然，M 是忠实的只是说表示 $\sigma:R\to\mathrm{End}_{\mathbb{Z}}(M)$（命题 8.8 中给出的）是一个单射．

称一个 R-模是**有限生成**的，如果存在有限个元素 $m_1,\cdots,m_n\in M$ 使得每个 $x\in M$ 都是 $m_1,\cdots,m_n$ 的一个 R-线性组合．特别地，称一个 R-模是**循环**的，如果它由一个元素生成．

例 8.9 设 E/k 是伽罗瓦扩张，它有伽罗瓦群 $G=\mathrm{Gal}(E/k)$，则 E 是一个 kG-模：如果 $e\in E$，则

$$\Big(\sum_{\sigma\in G}a_\sigma\sigma\Big)(e)=\sum_{\sigma\in G}a_\sigma\sigma(e).$$

如果 E 是一个循环 kG-模，我们说 E/k 有**正规基**．每个伽罗瓦扩张 E/k 都有正规基（见雅各布森所著的《Basic Algebra I》，283 页）． ■

现在我们可以讨论命题 7.24，即关于代数整数的一个较早的结果．

命题 8.10 （i）如果有限生成阿贝尔群 M 关于某个环 R 是忠实左 R-模，则 R 的加法群是有限生成的．

（ii）如果 α 是一个复数，令$\mathbb{Z}[\alpha]$ 是 α 生成的$\mathbb{C}$的子环．如果存在一个忠实$\mathbb{Z}[\alpha]$-模 M，而 M 作为阿贝尔群是有限生成的，则 α 是一个代数整数．

证明 （i）根据命题 8.8，环 R 同构于 $\mathrm{End}_{\mathbb{Z}}(M)$ 的一个子环．因 M 是有限生成的，习题 8.6 证明 $\mathrm{End}_{\mathbb{Z}}(M)=\mathrm{Hom}_{\mathbb{Z}}(M,M)$ 是有限生成的．根据命题 7.23，R 的加法群是有限生成的．

（ii）根据命题 7.24，只要证明环$\mathbb{Z}[\alpha]$ 作为阿贝尔群是有限生成的，这由（i）可得． ■

前面第 7 章中所有定义都可以对右边的版本定义——子模、商模、R-同态、同构定理、对应定理、直和等等——但有更优美的方法来定义．

528

定义 环 R 是一个有序三元组(R,α,μ)，其中 $\alpha:R\times R\to R$ 是加法，$\mu:R\times R\to R$ 是乘法，它

们满足特定的公理．两个环(R,α,μ)和(R',α',μ')是**相等的**，如果$R=R'$，$\alpha=\alpha'$，$\mu=\mu'$．定义**对立环**R^{op}为这样的环，它的加法群和R的加法群相同，而它的乘法$\mu^{op}:R\times R\to R$定义为$\mu^{op}(r,s)=\mu(s,r)=sr$.

这样，我们只是颠倒了乘法的次序．容易验证R^{op}是环，显然$(R^{op})^{op}=R$，此外，$R=R^{op}$当且仅当R是交换环．

命题 8.11 *每个右R-模M是一个左R^{op}-模，每个左R-模M是一个右R^{op}-模．*

证明 在这个证明中我们做得十分繁琐．说M是右R-模就是说存在函数$\sigma:M\times R\to M$，记为$\sigma(m,r)=mr$．如果$\mu:R\times R\to R$是R中给定的乘法，则右R-模定义中的公理（ⅲ）说

$$\sigma(m,\mu(r,r'))=\sigma(\sigma(m,r),r').$$

为了得到左R-模，定义$\sigma':R\times M\to M$为$\sigma'(r,m)=\sigma(m,r)$．为证明M是一个左R^{op}-模，只是一个验证公理（ⅲ）的问题，用繁琐记号来写就是

$$\sigma'(\mu^{op}(r,r'),m)=\sigma'(r,\sigma'(r',m)).$$

但

$$\sigma'(\mu^{op}(r,r'),m)=\sigma(m,\mu^{op}(r,r'))=\sigma(m,\mu(r',r))=m(r'r),$$

而右端是

$$\sigma'(r,\sigma'(r',m))=\sigma(\sigma'(r',m),r)=\sigma(\sigma(m,r'),r)=(mr')r.$$

这样，因M是右R-模，所以两端相等．

现在命题的第二部分随之可得，因为一个右R^{op}-模是一个左$(R^{op})^{op}$-模，也就是左R-模．■

由命题 8.11，关于左R-模的任意一个定理也是关于左R^{op}-模的定理，因此它也是关于右R-模的定理．

现在我们注意对立环不只是一种说明的方法，它们确实是自然地产生的．

命题 8.12 *如果把一个环看作它自身上的左模，则存在环同构*

$$\mathrm{End}_R(R)\cong R^{op}.$$

证明 定义$\varphi:\mathrm{End}_R(R)\to R^{op}$为$\varphi(f)=f(1)$，容易验证$\varphi$是加法阿贝尔群的同构．现在$\varphi(f)\varphi(g)=f(1)g(1)$．另一方面，$\varphi(fg)=(f\circ g)(1)=f(g(1))$．但如果记$r=g(1)$，则因$f$是一个$R$-映射，有$f(g(1))=f(r)=f(r\cdot 1)=rf(1)$，因此$f(g(1))=rf(1)=g(1)f(1)$．所以，

$$\varphi(fg)=\varphi(g)\varphi(f).$$

我们已经证明了$\varphi:\mathrm{End}_R(R)\to R$是加性双射，它颠倒了乘法次序．■ 529

一个**反同构**$\varphi:R\to A$，其中R和A都是环，是指一个加性双射满足

$$\varphi(rs)=\varphi(s)\varphi(r).$$

易知R和A是反同构的当且仅当$R\cong A^{op}$．例如$\mathbb{H}$中的共轭是一个反同构．如果k是交换环，则矩阵的转置$A\mapsto A^t$是一个反同构$\mathrm{Mat}_n(k)\to\mathrm{Mat}_n(k)$，这是因为$(AB)^t=B^tA^t$，所以$\mathrm{Mat}_n(k)\cong[\mathrm{Mat}_n(k)]^{op}$．然而当$k$不交换时，公式$(AB)^t=B^tA^t$不再成立．例如

$$\left(\begin{bmatrix}a&b\\c&d\end{bmatrix}\begin{bmatrix}p&q\\r&s\end{bmatrix}\right)^t=\begin{bmatrix}ap+br&aq+bs\\cp+dr&cq+ds\end{bmatrix}^t,$$

而

$$\begin{bmatrix} p & q \\ r & s \end{bmatrix}^t \begin{bmatrix} a & b \\ c & d \end{bmatrix}^t = \begin{bmatrix} p & r \\ q & s \end{bmatrix} \begin{bmatrix} a & c \\ b & d \end{bmatrix},$$

它们的 1,1 元素 $pa+rb \neq ap+br$.

命题 8.13 如果 R 是任意环，则

$$[\mathrm{Mat}_n(R)]^{\mathrm{op}} \cong \mathrm{Mat}_n(R^{\mathrm{op}}).$$

证明 我们断言转置 $A \mapsto A^t$ 是环同构

$$[\mathrm{Mat}_n(R)]^{\mathrm{op}} \to \mathrm{Mat}_n(R^{\mathrm{op}}).$$

首先，由 $(A^t)^t = A$ 知 $A \mapsto A^t$ 是双射．我们设置一些记号．如果 $M = [m_{ij}]$ 是矩阵，则它的 ij 元素 m_{ij} 也可以记为 $(M)_{ij}$．记 R^{op} 中的乘法为 $a * b$，其中 $a * b = ba$，并记 $[\mathrm{Mat}_n(R)]^{\mathrm{op}}$ 中的乘法为 $A * B$，其中 $(A * B)_{ij} = (BA)_{ij} = \sum_k b_{ik} a_{kj} \in R$．我们必须证明在 $\mathrm{Mat}_n(R^{\mathrm{op}})$ 中 $(A * B)^t = A^t B^t$. 在 $[\mathrm{Mat}_n(R)]^{\mathrm{op}}$ 中有

$$\begin{aligned} (A * B)^t_{ij} &= (BA)^t_{ij} \\ &= (BA)_{ji} \\ &= \sum_k b_{jk} a_{ki}. \end{aligned}$$

在 $\mathrm{Mat}_n(R^{\mathrm{op}})$ 中有

$$\begin{aligned} (A^t B^t)_{ij} &= \sum_k (A^t)_{ik} * (B^t)_{kj} \\ &= \sum_k (A)_{ki} * (B)_{jk} \\ &= \sum_k a_{ki} * b_{jk} \\ &= \sum_k b_{jk} a_{ki}. \end{aligned}$$

[530] 所以在 $\mathrm{Mat}_n(R^{\mathrm{op}})$ 中正如所要的有 $(A * B)^t = A^t B^t$. ∎

存在 R-模的直和与直积，其中 R 是任意环（不必交换）．毕竟一个 R-模是一个加法阿贝尔群配置了一个标量乘法．如果 $\{M_i : i \in I\}$ 是一族左 R-模，则作为基础阿贝尔群的直积来构造直积 $\prod_{i \in I} M_i$，然后定义标量乘法为 $r(m_i) = (rm_i)$，如果每个 M_i 都是左 R-模，而如果每个 M_i 都是右 R-模，则标量乘法定义为 $(m_i)r = (m_i r)$．和交换环上的模一样，定义直和 $\sum_{i \in I} M_i$ 为 $\prod_{i \in I} M_i$ 的子模，它由几乎一切坐标都为 0 的一切 I 元组组成．不难修改外直和与内直和的定义及其初等性质使它们适用于此，比如命题 7.15 和系 7.16.

因直和存在，我们也可以构造自由左 R-模（作为 ${}_R R$ 若干个复制的直和）和自由右 R-模（作为 R_R 的直和）．

左模或右模的正合列也有意义（也是因为模是具有额外结构的加法阿贝尔群），读者使用它们应该没有困难．

习题

8.1 设 R 是加法阿贝尔群，它配置一个结合的乘法，且满足两个分配律．定义阿贝尔群 $R^* = \mathbb{Z} \oplus R$ 上的乘法为

$$(m,r)(n,s)=(mn,ms+nr+rs),$$

其中当 $m>0$ 时，ms 是 m 个 s 的和，当 $m<0$ 时，ms 是 $|m|$ 个 $-s$ 的和．

证明 R^* 是有幺元 $(1,0)$ 的环，且 R 是 R^* 中的双边理想．（我们说 R^* 是在 R 中添加幺元得到的．）

8.2　设 R 是形如 $\begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix}$ 的一切矩阵的集合，其中 a，b 是复数，$\bar{a}$ 表示 a 的共轭复数．证明 R 是 $\mathrm{Mat}_2(\mathbb{C})$ 的子环，且 $R\cong\mathbb{H}$，其中 $\mathbb{H}$ 是四元数除环．

8.3　证明在环 R 上下列条件等价：

（ⅰ）对每个左理想的序列 $L_1\supseteq L_2\supseteq L_3\supseteq\cdots$，存在 N 使得当 $i\geqslant N$ 时有 $L_i=L_{i+1}$；

（ⅱ）左理想的每个非空族 $\mathcal{F}$ 都有极小元素．

8.4　**（环的转变）** 设 $\varphi: R\to S$ 是环同态，并设 M 是左 S-模．证明由 $(r,m)\mapsto\varphi(r)m$ 给出的函数 $R\times M\to M$ 定义了一个标量乘法，使得 M 成为左 R-模．

8.5　设 I 是环 R 中的双边理想．证明一个阿贝尔群 M 是一个左 (R/I)-模当且仅当 M 是被 I 零化的左 R-模．

8.6　如果 M 是有限生成的阿贝尔群，证明环 $\mathrm{End}(M)$ 的加法群是有限生成的阿贝尔群．

531

提示：存在映射到 M 上的有限生成自由阿贝尔群 F，把 $\mathrm{Hom}(\ ,M)$ 作用到 $F\to M\to 0$ 上以获得一个单射 $0\to\mathrm{Hom}(M,M)\to\mathrm{Hom}(F,M)$．但 $\mathrm{Hom}(F,M)$ 是 M 的若干个复制的有限直和．

8.7　（ⅰ）如果 k 是交换环，G 是有有限阶 n 的循环群，证明 $kG\cong k[x]/(x^n-1)$．

（ⅱ）如果 k 是整环，定义**洛朗多项式环**为 $k(x)$ 的子环，它由一切形如 $f(x)/x^n$ 的有理函数组成，其中 $n\in\mathbb{Z}$．如果 G 是无限循环群，证明 kG 同构于洛朗（Laurent）多项式．

8.8　设 R 是 $\mathbb{C}$ 上的四维向量空间，基为 $1,i,j,k$．在 R 上定义一个乘法，使得基元素满足四元数 $\mathbb{H}$ 中满足的那些恒等式［见例 8.1(ⅵ)］．证明 R 不是除环．

8.9　如果 k 是环，可以不交换，证明 $\mathrm{Mat}_n(k)$ 是环．

8.10　证明矩阵环 $\mathrm{Mat}_n(R)$ 的中心是一切标量矩阵 aI 的集合，其中 $a\in Z(R)$，I 是单位矩阵．

8.11　证明 $Z(\mathbb{H})=\{a1 : a\in\mathbb{R}\}$．

8.12　设 $R=R_1\times\cdots\times R_m$ 是环的直积．

（ⅰ）证明 $R^{\mathrm{op}}=R_1^{\mathrm{op}}\times\cdots\times R_m^{\mathrm{op}}$．

（ⅱ）证明 $Z(R)=Z(R_1)\times\cdots\times Z(R_m)$．

（ⅲ）如果 k 是域且

$$R=\mathrm{Mat}_{n_1}(k)\times\cdots\times\mathrm{Mat}_{n_m}(k),$$

证明 $\dim_k(Z(R))=m$．

8.13　如果 Δ 是除环，证明 Δ^{op} 也是除环．

8.14　环 A 中的一个**幂等元**是指满足 $e^2=e$ 的元素 $e\in A$．如果 R 是环，M 是左 R-模，证明每个直和项 $S\subseteq M$ 确定 $\mathrm{End}_R(M)$ 中的一个幂等元．

提示：见系 7.17.

8.15　设 R 是环．

（ⅰ）**（皮尔斯分解）** 证明：如果 e 是环 R 中的幂等元，则

$$R=Re\oplus R(1-e).$$

（ⅱ）设 R 是环，它有左理想 I,J 使得 $R=I\oplus J$．证明存在幂等元 $e\in I$ 和 $f\in J$ 使得 $1=e+f$．此外，$I=Ie$，$J=Jf$．

提示：分解 $1=e+f$，并证明 $ef=0=fe$．

8.16　称环 R 中的元素 a 有左逆，如果存在 $u\in R$ 使得 $ua=1$．称 a 有右逆，如果存在 $w\in R$ 使得 $aw=1$．

(i) 证明：如果 $a \in R$ 既有左逆 u 又有右逆 w，则 $u = w$.

(ii) 举出一个环 R 的例子，其中一个元素 a 有两个不同的左逆.

提示：定义 $R = \mathrm{End}_k(V)$，其中 V 是域 k 上的向量空间，且有基 $\{b_n : n \geqslant 1\}$，定义 $a \in R$ 为对一切 $n \geqslant 1$，$a(b_n) = b_{n+1}$.

(iii)（**卡普兰斯基**）设 R 是环，并设 $a,u,v \in R$ 满足 $ua = 1 = va$. 如果 $u \neq v$，证明 a 有无限个左逆.

提示：元素 $u + a^n(1-au)$ 是不同的吗？

532 8.17 设 k 是域，G 是有限群，并设 $\mathcal{F}(G,k)$ 表示 $G \to k$ 的一切函数的向量空间.

(i) 定义 $\varphi : kG \to \mathcal{F}(G,k)$ 如下：如果 $u = \sum_x a_x x \in kG$，则 $\varphi_u : x \mapsto a_x$. 证明

$$\varphi_{u+v} = \varphi_u + \varphi_v$$

和

$$\varphi_{uv}(y) = \sum_{x \in G} \varphi_u(x)\varphi_v(x^{-1}y).$$

（上面的算子叫做 φ_u 和 φ_v 的**卷积**.）

(ii) 证明 $\mathcal{F}(G,k)$ 是环，由 $u \mapsto \varphi_u$ 给出的 $\mathcal{F} : kG \to \mathcal{F}(G,k)$ 是环同构.

8.18 (i) 对域 k 和有限群 G，证明 $(kG)^{\mathrm{op}} \cong kG$.

(ii) 证明 $\mathbb{H}^{\mathrm{op}} \cong \mathbb{H}$，其中 $\mathbb{H}$ 是实四元数除环.

习题 8.30 要找不同构于 R^{op} 的环 R.

8.19 (i) 如果 R 是环，$r \in R$，又如果 $k \subseteq Z(R)$ 是子环，证明由 r 和 k 生成的子环是交换的.

(ii) 如果 Δ 是除环，$r \in \Delta$，又如果 $k \subseteq Z(\Delta)$ 是子环，证明由 r 和 k 生成的子除环是（交换）域.

8.20 记四元数群 $\mathbf{Q}$ 的元素为

$$1, \bar{1}, i, \bar{i}, j, \bar{j}, k, \bar{k},$$

定义线性变换 $\varphi : \mathbb{R}\mathbf{Q} \to \mathbb{H}$ 为移开横：

$$\text{对 } x = 1, i, j, k,\ \varphi(\bar{x}) = \varphi(x) = x.$$

证明 φ 是满射环映射，由此推出存在环同构 $\mathbb{R}\mathbf{Q}/\ker\varphi \cong \mathbb{H}$.（较少计算的证明见例 9.113.）

8.21 如果 R 是环，其中对每个 $x \in R$ 有 $x^2 = x$，证明 R 是交换环.（布尔环是这种环的一个例子.）

8.22 证明存在范畴 ${}_R\mathbf{Mod} \to \mathbf{Mod}_{R^{\mathrm{op}}}$ 的等价.

提示：给定左 R-模 (M,σ)，其中 M 是一个加法阿贝尔群，$\sigma : R \times M \to M$ 是标量乘法，考虑右 R^{op}-模 (M,σ')，其中 $\sigma' : M \times R^{\mathrm{op}} \to M$ 由命题 8.11 定义. 定义 $F : {}_R\mathbf{Mod} \to \mathbf{Mod}_{R^{\mathrm{op}}}$ 在对象上是 $(M,\sigma) \mapsto (M,\sigma')$.

8.2 链条件

本节介绍任意环上模的链条件，以及雅各布森根 $J(R)$，它是一个对环 R 有影响的双边理 533 想. 例如，半单环 R 是有限群 G 的群环 $\mathbb{C}G$ 的推广，在下一节中，要用 $J(R)$ 和链条件刻画它们. 我们还要证明韦德伯恩（Wedderburn）的一个定理，该定理说有限除环是域，也就是它是交换的.

我们已经证明了群的若尔当-赫尔德定理（见定理 5.52），这里有这个定理关于模的版本. 如果引入算子群的概念，则可以同时证明这两个版本（见 Robinson 所著的《A Course in the Theory of Groups》65 页）.

定理 8.14（扎森豪斯引理） *给定模 M（在任意环上）的子模 $A \subseteq A^*$ 和 $B \subseteq B^*$，存在同构*

$$\frac{A+(A^*\cap B^*)}{A+(A^*\cap B)}\cong\frac{B+(B^*\cap A^*)}{B+(B^*\cap A)}.$$

证明　引理 5.49 的证明经简单修改就适用于此．■

定义　模 M（在任意环上）的一个**列**（或一个**过滤**）是指子模的有限序列 $M=M_0,M_1,M_2,\cdots,M_n=\{0\}$，它满足

$$M=M_0\supseteq M_1\supseteq M_2\supseteq\cdots\supseteq M_n=\{0\}.$$

这个列的**因子模**是指模 $M_0/M_1,M_1/M_2,\cdots,M_{n-1}/M_n=M_{n-1}$，**长度**是指严格包含关系的个数，等价地说，长度是非零因子模的个数．

列的一个**加细**是指以原来的列作为子序列的列 $M=M_0',M_1',\cdots,M_k'=\{0\}$．称模 M 的两个列**等价**，如果在两个非零因子模的集合间存在双射使得对应的因子模同构．

定理 8.15（施赖埃尔加细定理）　模 M 的任意两个列

$$M=M_0\supseteq M_1\supseteq\cdots\supseteq M_n=\{0\}\text{ 和 }M=N_0\supseteq N_1\supseteq\cdots\supseteq N_k=\{0\}$$

有等价的加细．

证明　定理 5.51 的证明经简单修改就适用于此．■

定义　称一个左 R-模是**单模**（或**不可约**），如果 $M\neq\{0\}$ 且 M 没有真子模．

和交换环上的模一样，对应定理表明模 M 的一个 R-子模是极大子模当且仅当 M/N 是单模．可以修改系 7.14 的证明来证明一个左 R-模 S 是单模当且仅当 $S\cong R/I$，其中 I 是极大左理想．[534]

定义　**合成列**是指一切非零因子模都是单模的列．

注意一个合成列只允许有无意义的加细，也就是只能重复它的项（如果 M_i/M_{i+1} 是单模，则 M_i/M_{i+1} 没有非零真子模，因此没有中间子模 L 能够满足 $M_i\supsetneq L\supsetneq M_{i+1}$）．精确地说，合成列的任一加细等价于原来的合成列．

一个模未必有合成列，例如把阿贝尔群$\mathbb{Z}$看作$\mathbb{Z}$-模就没有合成列．

定义　任意环 R 上的一个左 R-模 M 称为**有升链条件**，缩写为 ACC，如果每个左子模的升链都**有终止**：如果

$$S_1\subseteq S_2\subseteq S_3\subseteq\cdots$$

是子模的链，则存在某个 $t\geqslant 1$ 使得

$$S_t=S_{t+1}=S_{t+2}=\cdots.$$

任意环 R 上的一个左 R-模称为**有降链条件**，缩写为 DCC，如果每个左子模的降链都**有终止**：如果

$$S_1\supseteq S_2\supseteq S_3\supseteq\cdots$$

是子模的链，则存在某个 $t\geqslant 1$ 使得

$$S_t=S_{t+1}=S_{t+2}=\cdots.$$

第 6 章中对交换诺特环证明的大多数定理（例如命题 6.38：ACC、极大条件和理想的有限生成之间的等价）都能够推广到有 ACC 的左模，证明也相同．

命题 8.16　（ⅰ）如果一个左模 M 有 DCC，则子模的每个非空族$\mathcal{F}$包含一个极小元素，即存在子模 $S_0\in\mathcal{F}$，使得没有一个 $S\in\mathcal{F}$能够满足 $S\subsetneq S_0$．

（ⅱ）如果一个左模 M 有 ACC，则子模的每个非空族$\mathcal{F}$包含一个极大元素，即存在子模 $S_0\in\mathcal{F}$，使得没有一个 $S\in\mathcal{F}$能够满足 $S\supsetneq S_0$．

证明　选取 $S\in\mathcal{F}$．如果 S 是$\mathcal{F}$的极小元素，证明已经完成．否则，存在子模 $S_1\in\mathcal{F}$使得 $S\supsetneq S_1$．如果 S_1 是极小元素，证明已经完成．否则，存在子模 $S_2\in\mathcal{F}$使得 $S\supsetneq S_1\supsetneq S_2$．DCC 说这个序列

必终止，即存在 $S_t\in\mathcal{F}$，它是$\mathcal{F}$的极小元素（因为寻找一个更小子模的阻碍只有 S_t 是极小元素）.
535 第二个陈述的证明类似． ■

命题 8.17 任意环 R 上的模 M 有合成列当且仅当它有关于子模的两个链条件．

证明 如果 M 有长度为 n 的合成列，则没有一个子模序列的长度 $>n$，否则就要违背施赖埃尔定理（加细一个列不可能缩短它）．所以 M 有两个链条件．

设$\mathcal{F}_1$ 是 M 的一切真子模的族．根据命题 8.16，极大条件给出极大子模 $M_1\in\mathcal{F}_1$．设$\mathcal{F}_2$ 是 M_1 的一切真子模的族，并设 M_2 是这种极大子模．迭代得递减序列

$$M\supsetneq M_1\supsetneq M_2\supsetneq\cdots.$$

如果 M_n 出现在这个序列中，则阻碍构造 M_{n+1} 的只有 $M_n=0$. 因 M 有两个链条件，这个链必终止，所以有某个 t 使得 $M_t=0$. 这个链就是 M 的合成列，这是因为每个 M_i 都是它前一个的极大子模． ■

定理 8.18（若尔当-赫尔德定理） 模 M 的任意两个合成列等价．特别地，如果合成列存在，则合成列的长度是 M 的不变量，叫做 M 的**长度**．

证明 前面我们注明合成列的任一加细等价于原来的合成列，现在由施赖埃尔定理，任意两个合成列等价，特别地，它们有相同的长度． ■

设 V 是域 k 上的向量空间，如果 V 的维数为 n，则 V 有基 $v_1,\cdots,v_n$，它的一个合成列是

$$V=\langle v_1,\cdots,v_n\rangle\supsetneq\langle v_2,\cdots,v_n\rangle\supsetneq\cdots\supsetneq\langle v_n\rangle\supsetneq\{0\}$$

（因子模是一维的，因此是单 k-模），所以 V 的长度为 n.

系 8.19 如果模 M 的长度为 n，则每个 M 的子模的链的长度 $\leqslant n$.

证明 根据施赖埃尔定理，给定的链可以加细成一个合成列，所以给定链的长度最多为 n. ■

若尔当-赫尔德定理可以看作一种唯一因子分解定理，例如我们在系 5.53 中看到它给出了算术基本定理的一个新证明．

如果 Δ 是除环，则一个左 Δ-模叫做 Δ 上的一个**左向量空间**. 下面的来自线性代数的定义在这里仍然有意义．

定义 如果 V 是除环 Δ 上的一个左向量空间，则 V 中的表 $X=x_1,\cdots,x_m$ 称为**线性相关**，如果有某个 i 使得

$$x_i\in\langle x_1,\cdots,\hat{x}_i,\cdots,x_m\rangle;$$

536 否则称 X 为**线性无关**．

读者应验证：如果 $x_1,\cdots,x_m$ 线性无关，则

$$\langle x_1,\cdots,x_m\rangle=\langle x_1\rangle\oplus\cdots\oplus\langle x_m\rangle.$$

命题 8.20 除环 Δ 上的每个有限生成左向量空间 $V=\langle v_1,\cdots,v_n\rangle$ 都是若干个 Δ 复制的直和；即一个除环上的每个有限生成左向量空间都有基．

证明 考虑列

$$V=\langle v_1,\cdots,v_n\rangle\supseteq\langle v_2,\cdots,v_n\rangle\supseteq\langle v_3,\cdots,v_n\rangle\supseteq\cdots\supseteq\langle v_n\rangle\supseteq\{0\}.$$

记$\langle v_{i+1},\cdots,v_n\rangle$为 U_i，从而$\langle v_i,\cdots,v_n\rangle=\langle v_i\rangle+U_i$. 根据第二同构定理，

$$\langle v_i,\cdots,v_n\rangle/\langle v_{i+1},\cdots,v_n\rangle=(\langle v_i\rangle+U_i)/U_i\cong\langle v_i\rangle/(\langle v_i\rangle\cap U_i).$$

所以第 i 个因子模同构于$\langle v_i\rangle$的一个商，而如果 $v_i\neq 0$，则$\langle v_i\rangle\cong\Delta$. 因 Δ 是除环，它的商只有 Δ 和 $\{0\}$．抛弃对应于平凡因子模 $\{0\}$ 的那些 v_i，我们断言剩下的那些 v（记为 $v_1,\cdots,v_m$）组成基. 对一

切 j，有 $v_j \notin \langle v_{j+1},\cdots,v_n\rangle$. 读者现在可以对 m 用归纳法证明$\langle v_1\rangle$，…，$\langle v_m\rangle$生成一个直和．■

这个命题的另一个证明使用了相关关系，在习题 8.23（ⅱ）中有概要叙述．

下一个问题是 V 的任意两个基是否有相同的元素个数．实际情况是关于域上向量空间的定理与除环上的左向量空间的定理十分相似，但读者不应轻率地加以接受．

系 8.21 *如果 V 是除环 Δ 上有限生成的左向量空间，则 V 的任意两个基有相同的元素个数．*

证明 和命题 8.20 的证明一样，V 的一个基给出一个列

$$V=\langle v_1,v_2,\cdots,v_n\rangle \supsetneq \langle v_2,\cdots,v_n\rangle \supsetneq \langle v_3,\cdots,v_n\rangle \supsetneq \cdots \supsetneq \langle v_n\rangle \supsetneq \{0\}.$$

因为每个因子模同构于 Δ，而 Δ 是除环，因此是单的，从而这个列是合成列．根据若尔当-赫尔德定理，由 V 的任意其他的基形成的合成列必有相同的长度．■

这个系的另一个证明在习题 8.23（ⅲ）中有概要叙述．

由此，一个除环 Δ 上的有限生成左向量空间有左维数，我们把它记为 $\dim(V)$.

如果一个阿贝尔群 V 既是一个除环 Δ 上的左向量空间又是右向量空间，那么它的左维数一定等于它的右维数吗？有一个除环 Δ 和一个阿贝尔群 V 的例子，它是 Δ 上的双侧向量空间，左维数为 2，而右维数为 3.（见 Jacobson 所著的《Structure of Rings》158 页．）

537

我们刚才已经看到除环上的左向量空间的维数是合理定义的．对每个环 R，一个自由左 R-模 F 的秩是合理定义的吗？即 F 的任意两个基有相同的元素个数吗？在命题 7.50 中，我们看到当 R 是交换环时，秩是合理定义的，可以证明当 R 是左诺特环时，即 R 中的每个左理想都有限生成的，秩也是合理定义的（见 Rotman 所著的《An Introduction to Homological Algebra》111 页）．然而，下一个例子表明秩不总是合理定义的．

例 8.22 设 k 是域，V 是 k 上有无限基 $\{v_n : n\in \mathbb{N}\}$ 的向量空间，并设 $R=\mathrm{End}_k(V)$．设 A 是由满足对一切 n 有 $\varphi(v_{2n})=0$ 的一切线性变换 $\varphi: V\to V$ 组成的左理想，又设 B 是由满足对一切 n 有 $\psi(v_{2n+1})=0$ 的一切线性变换 $\psi: V\to V$ 组成的左理想．我们让读者验证 $A\cap B=\{0\}$ 且 $A+B=R$，从而 $R=A\oplus B$．

设 W 是以奇数下标的 v_{2n+1} 为基的 V 的子空间．如果 $f: V\to W$ 是一个 k-同构，则映射 $\psi\mapsto f\psi f^{-1}$ 是 R-同构

$$R=\mathrm{End}_k(V)\cong \mathrm{End}_k(W)=A.$$

同样，如果 Y 是由偶数下标的 v_{2n} 张成的 V 的子空间，则 $R\cong \mathrm{End}_k(V)=B$．由此，自由左 R-模 R 和 $R\oplus R$ 同构．■

有另一个有用的因子分解定理．任意环 R 上的一个左 R-模 M 称为**不可分解模**，如果不存在非零子模 A 和 B 使得 $M=A\oplus B$．**克鲁尔-施密特**定理说，如果 M 有关于子模的两个链条件，则 M 是不可分解模的直和：$M=A_1\oplus\cdots\oplus A_n$．此外，如果 $M=B_1\oplus\cdots\oplus B_m$ 是另一个分解为不可分解模的分解，则 $m=n$，且存在置换 $\sigma\in S_n$ 使得对一切 i 有 $A_i\cong B_{\sigma(i)}$．证明可在 Rotman 所著的《An Introduction to the Theory of Groups》144～150 页中找到．

下面是韦德伯恩的一个惊奇的结果．

定理 8.23（韦德伯恩） *有限除环 D 是域；即 D 中的乘法是交换的．*

证明（维特[⊖]） 如果记 D 的中心为 Z，则 Z 是有限域，因此它有 q 个元素（其中 q 是某个素数的幂）．由此 D 是 Z 上的向量空间，从而有某个 $n\geqslant 1$ 使得 $|D|=q^n$；即如果我们定义

⊖ 在定理 9.123 中我们将给出另一个证明．

$$[D:Z]=\dim_Z(D),$$

则 $[D:Z]=n$. 如果能够证明 $n>1$ 将导致矛盾，就能完成证明.

如果 $a\in D$，定义 $C(a)=\{u\in D: ua=au\}$. 容易验证 $C(a)$ 是包含 Z 的 D 的子除环：如果 u,v 538 $\in D$ 与 a 可交换，则 $u+v,uv$ 和 u^{-1}（当 $u\neq 0$ 时）也与 a 可交换. 由此，有某个整数 $d(a)$ 使得 $|C(a)|=q^{d(a)}$，即$[C(a):Z]=d(a)$. 我们不知道 $C(a)$是否可交换，但习题 8.25 给出

$$[D:Z]=[D:C(a)][C(a):Z],$$

其中$[D:C(a)]$表示 D 的作为$C(a)$上的左向量空间的维数. 即 $n=[D:C(a)]d(a)$,从而 $d(a)$是 n 的因数.

因 D 是除环，它的非零元素 $D^\times$ 形成 q^n-1 阶乘法群. 根据例 8.2 (ii)，群 $D^\times$ 的中心是 $Z^\times$，并且如果 $a\in D^\times$，则它的中心化子 $C_{D^\times}(a)=C(a)^\times$. 因此，$|Z(D^\times)|=q-1$和 $|C_{D^\times}(a)|=q^{d(a)}-1$，其中 $d(a)\mid n$.

$D^\times$ 的类方程是

$$|D^\times|=|Z^\times|+\sum_i[D^\times:C_{D^\times}(a_i)],$$

其中从每个非中心的共轭类中选取一个 a_i. 但

$$[D^\times:C_{D^\times}(a_i)]=|D^\times|/|C_{D^\times}(a_i)|=(q^n-1)/(q^{d(a_i)}-1),$$

从而类方程变成

$$q^n-1=q-1+\sum_i\frac{q^n-1}{q^{d(a_i)}-1}. \tag{1}$$

我们已经注意到每个 $d(a_i)$都是 n 的因数，而 a_i 不在中心的条件说明 $d(a_i)<n$.

回忆 n 阶分圆多项式是 $\Phi_n(x)=\prod(x-\zeta)$，其中 ζ 遍历一切 n 次单位原根. 在系 1.41 中，我们证明对一切 i，$\Phi_n(q)$是 q^n-1和$(q^n-1)/(q^{d(a_i)}-1)$的公因数，因此等式 (1) 给出

$$\Phi_n(q)\mid(q-1).$$

如果 $n>1$ 且 ζ 是 n 次单位原根，则 $\zeta\neq 1$，因此 ζ 是单位圆上的其他点. 因 q 是素数幂，它是 x-轴上的一个点，且 $q\geqslant 2$，从而距离 $|q-\zeta|>q-1$. 所以

$$|\Phi_n(q)|=\prod|q-\zeta|>q-1,$$

这与 $\Phi_n(q)\mid(q-1)$矛盾. 由此可知，$n=1$，即 $D=Z$，因此 D 是交换的. ■

接下来的讨论将用在下一节中证明韦德伯恩-阿廷关于半单环分类的定理. 考虑 $\mathrm{Hom}_R(A,B)$，其中 A,B 都是左 R-模，且都是有限直和：比如 $A=\sum_{i=1}^n A_i, B=\sum_{j=1}^m B_j$. 根据定理 7.32 和定理 7.33，有

539

$$\mathrm{Hom}_R(A,B)\cong\sum_{ij}\mathrm{Hom}_R(A_i,B_j).$$

精确地说，如果 $\alpha_i: A_i\to A$ 是第 i 个内射，且 $p_j: B\to B_j$ 是第 j 个投射，则每个 $f\in\mathrm{Hom}_R(A,B)$给出映射 $f_{ij}=p_jf\alpha_i\in\mathrm{Hom}_R(A_i,B_j)$. 于是，$f$ 定义了一个 $n\times m$ **广义矩阵**$[f_{ij}]$（我们称 $[f_{ij}]$ 是一个广义矩阵，因为不同位置的元素未必在同一个代数系统中）. 映射 $f\mapsto[f_{ij}]$是同构 $\mathrm{Hom}_R(A,B)\to\sum_{ij}\mathrm{Hom}_R(A_i,B_j)$. 同样，如果 $g: B\to C$，其中 $C=\sum_{k=1}^{\ell}C_k$，则 g 定义了一个广义 $m\times\ell$ 矩阵$[g_{jk}]$，其中 $g_{jk}=q_kg\beta_j: B_j\to C_k$，$\beta_j: B_j\to B$ 是内射，$q_k: C\to C_k$ 是投射.

复合 $gf: A\to C$ 定义了一个广义 $n\times\ell$ 矩阵，我们断言这个矩阵由矩阵乘法 $(gf)_{ik}=\sum_j g_{kj}f_{ji}$

给出：因为 $\sum_j \beta_j p_j = 1_B$，所以有

$$\begin{aligned}\sum_j g_{kj} f_{ji} &= \sum_j q_k g \beta_j p_j f \alpha_i \\ &= q_k g \left(\sum_j \beta_j p_j\right) f \alpha_i \\ &= q_k g f \alpha_i \\ &= (gf)_{ik}.\end{aligned}$$

附加某些假设，我们可以把广义矩阵变成真正的矩阵．

命题 8.24 设 $V = \sum_{i=1}^{n} V_i$ 是左 R-模．如果存在左 R-模 L，且对每个 i 存在同构 $\varphi_i : V_i \to L$，则存在环同构

$$\mathrm{End}_R(V) \cong \mathrm{Mat}_n(\mathrm{End}_R(L)).$$

证明 定义

$$\theta : \mathrm{End}_R(V) \to \mathrm{Mat}_n(\mathrm{End}_R(L))$$

为

$$\theta : f \mapsto [\varphi_j p_j f \alpha_i \varphi_i^{-1}],$$

其中 $\alpha_i : V_i \to V$ 和 $p_j : V \to V_j$ 分别是内射和投射．θ 为加性同构是因为恒等式

$$\mathrm{Hom}\left(\sum_i V_i, \sum_i V_i\right) \cong \sum_{ij} \mathrm{Hom}(V_i, V_j),$$

当指标集有限时成立．在讨论广义矩阵时，位于 ij 的元素在 $\mathrm{Hom}_R(V_i, V_j)$ 中，而现在这些元素都在同构仿样 $\mathrm{Hom}_R(L, L) = \mathrm{End}_R(L)$ 中．

现在证明 θ 保持乘法．如果 $g, f \in \mathrm{End}_R(V)$，则 $\theta(gf) = [\varphi_j p_j g f \alpha_i \varphi_i^{-1}]$，而矩阵乘积是 [540]

$$\begin{aligned}\theta(g)\theta(f) &= \left[\sum_k (\varphi_j p_j g \alpha_k \varphi_k^{-1})(\varphi_k p_k f \alpha_i \varphi_i^{-1})\right] \\ &= \left[\sum_k \varphi_j p_j g \alpha_k p_k f \alpha_i \varphi_i^{-1}\right] \\ &= \left[\varphi_j p_j g \left(\sum_k \alpha_k p_k\right) f \alpha_i \varphi_i^{-1}\right] \\ &= [\varphi_j p_j g f \alpha_i \varphi_i^{-1}].\end{aligned}$$

系 8.25 如果 V 是除环 Δ 上的 n 维左向量空间，则存在环同构：

$$\mathrm{End}\Delta(V) \cong \mathrm{Mat}_n(\Delta)^{\mathrm{op}}.$$

证明 同构 $\mathrm{End}_k(V) \cong \mathrm{Mat}_n(\Delta^{\mathrm{op}})$ 是命题 8.24 对于 $V = V_1 \oplus \cdots \oplus V_n$ 的特殊情形，其中每个 V_i 是一维的，因此同构于 Δ．注意，根据命题 8.12，$\mathrm{End}_\Delta(\Delta) \cong \Delta^{\mathrm{op}}$．现在运用命题 8.13，它说 $\mathrm{Mat}_n(\Delta^{\mathrm{op}}) \cong \mathrm{Mat}_n(\Delta)^{\mathrm{op}}$． ■

下一结果涉及一种直和分解，它是和命题 8.24 中的分解相对立的一个极端情形．

系 8.26 设 R-模 M 是直和 $M = B_1 \oplus \cdots \oplus B_m$，其中对一切 $i \neq j$，$\mathrm{Hom}_R(B_i, B_j) = \{0\}$．则存在环同构

$$\mathrm{End}_R(M) \cong \mathrm{End}_R(B_1) \times \cdots \times \mathrm{End}_R(B_m).$$

证明 如果 $f, g \in \mathrm{End}_R(M)$，令 $[f_{ij}]$ 和 $[g_{ij}]$ 是它们的广义矩阵．只要证明 $[g_{ij}][f_{ij}]$ 是对角矩阵

$$\mathrm{diag}(g_{11}f_{11},\cdots,g_{mm}f_{mm}).$$

而当 $i\neq j$ 时，$g_{ik}f_{kj}\in \mathrm{Hom}_R(B_i,B_j)=0$，因此 $(gf)_{ij}=\sum_k g_{ik}f_{kj}=0$． ■

定义 假定 k 是交换环，则环 R 称为 **k-代数**，如果 R 是一个 k-模，且 k 中的标量和每一个都可交换：对一切 $a\in k$ 和 $r,s\in R$，

$$a(rs)=(ar)s=r(as).$$

假定 R 和 S 都是 k-代数，则环同态 $f:R\to S$ 称为 **k-代数映射**，如果对一切 $a\in k$ 和 $r\in R$，

$$f(ar)=af(r),$$

541 即 f 也是 k-模映射．

k 被假定为交换环（在 k-代数的定义中）的理由可以在一个重要的特殊情形中看到，如果 k 是 R 的子环，令 $s=1$ 并取 $r\in k$，则有 $ar=ra$.

例 8.27 （ⅰ）如果 $A=\mathbb{C}[x]$，则 A 是$\mathbb{C}$-代数，且由 $\varphi:\sum_j c_jx^j\mapsto\sum_j c_j(x-1)^j$ 定义的 $\varphi:A\to A$ 是$\mathbb{C}$-代数映射．另一方面，由 $\theta:\sum_j c_jx^j\mapsto\sum_j \bar{c}_j(x-1)^j$（其中 $\bar{c}$ 是 c 的共轭复数）定义的函数 $\theta:A\to A$ 是环映射，但不是$\mathbb{C}$代数映射．例如，$\theta(ix)=-i(x-1)$，而 $i\theta(x)=i(x-1)$．现在$\mathbb{C}[x]$ 也是$\mathbb{R}$-代数，θ 是$\mathbb{R}$-代数映射．

（ⅱ）每个环 R 都是一个$\mathbb{Z}$-代数，且每个环同态都是一个$\mathbb{Z}$-代数映射．这个例子表明在 R-代数的定义中为什么不要求 k 同构于 R 的子环．

（ⅲ）如果 k 是包含于 R 的中心内的子环，则 R 是 k-代数．

（ⅳ）如果 k 是交换环，则 $\mathrm{Mat}_n(k)$ 是 k-代数．

（ⅴ）如果 k 是交换环，G 是群，则群代数 kG 是 k-代数． ■

我们现在已经对任意环的左模定义了 ACC. 下一定义说，环 R 是左诺特环，如果把它看作自身上的左模时有 ACC（回忆它的子模是左理想）．早先诺特环的定义是这里当 R 交换时的特殊情形．

定义 称环 R 为**左诺特环**，如果它有左理想的 **ACC（升链条件）**：每个左理想的升链

$$I_1\subseteq I_2\subseteq I_3\subseteq\cdots$$

都有终止；即存在某个 $t\geqslant 1$ 使得

$$I_t=I_{t+1}=I_{t+2}=\cdots.$$

类似定义**右诺特环**为有右理想的 ACC 的环．如果 k 是域，则每个有限维 k-代数 A 既是左诺特环又是右诺特环，这是因为当 $\dim(A)=n$ 时，任一左理想的升链或右理想的升链最多有 n 个严格包含关系．特别地，如果 G 是有限群，则 kG 的维数有限，因此它既是左诺特环又是右诺特环．习题 8.28 给出一个左诺特环的例子，它不是右诺特环．

命题 8.28 在环 R 上下面的条件等价：

（ⅰ）R 是左诺特环．

（ⅱ）R 的每个左理想的非空族包含极大元素．

542 （ⅲ）每个左理想都是有限生成的．

证明 修改命题 6.38 的证明即可． ■

定义 称环 R 为**左阿廷环**，如果它有 **DCC（降链条件）**：每个左理想的降链

$$I_1\supseteq I_2\supseteq I_3\supseteq\cdots$$

都有终止；即存在某个 $t\geqslant 1$ 使得

$$I_t = I_{t+1} = I_{t+2} = \cdots.$$

类似定义**右阿廷环**，有非右阿廷环的左阿廷环的例子（见习题 8.29）．如果 k 是域，则每个有限维 k-代数 A 既是左阿廷环又是右阿廷环，这是因为当 $\dim(A)=n$ 时，任一左理想或右理想的降链最多有 n 个严格包含关系．特别地，如果 G 是有限群，则 kG 的维数有限，因此它既是左阿廷环又是右阿廷环．由此可知，当 k 是域而 G 是有限群时，kG 有两个链条件（左侧和右侧）.

环 $\mathbb{Z}$ 是（左）诺特环，但不是（左）阿廷环，因为链

$$\mathbb{Z} \supsetneq (2) \supsetneq (2^2) \supsetneq (2^3) \supsetneq \cdots$$

没有终止．下一节中，我们要证明一个环是左阿廷环蕴涵它是左诺特环．

定义　环 R 中的左理想 L 称为**极小左理想**，如果 $L \neq \{0\}$ 且没有左理想 J 能够满足 $\{0\} \subsetneq J \subsetneq L$.

一个环未必含有极小左理想．例如 $\mathbb{Z}$ 就没有极小理想：$\mathbb{Z}$ 中每个非零理想 I 都有 $I=(n)$ 的形式，其中 n 是某个非零整数，而 $I=(n) \supsetneq (2n)$.

命题 8.29　（ⅰ）环 R 中的每个极小左理 L 都是单左 R-模．

（ⅱ）如果 R 是左阿廷环，则每个非零左理想 I 包含极小左理想．

证明　（ⅰ）如果 L 包含子模 S 满足 $\{0\} \subsetneq S \subsetneq L$，则 S 是 R 的左理想，与 L 的极小性矛盾．

（ⅱ）如果 $\mathcal{F}$ 是一切包含在 I 内的非零左理想的族，则因 I 是非零的，所以 $\mathcal{F} \neq \varnothing$. 根据命题 8.16，$\mathcal{F}$ 有极小元素，这样的元素就是极小左理想．■

我们现在定义一种特殊的理想，它由雅各布森引入，类似于群论中的弗拉蒂尼（Fratini）子群．　543

定义　如果 R 是环，定义它的**雅各布森根** $J(R)$ 为 R 中一切极大左理想的交．如果 $J(R)=\{0\}$，则称环 R 为**雅各布森半单环**．

显然，我们可以定义另一种雅各布森根：一切极大右理想的交．然而，这两种根是相同的（见命题 8.36）．

环 $\mathbb{Z}$ 是雅各布森半单的．$\mathbb{Z}$ 中的极大理想是非零素理想 (p)，因此 $J(\mathbb{Z}) = \bigcap_{\text{素数}\,p} (p) = \{0\}$. 如果 R 是*局部环*（有唯一极大理想 P 的交换环），则 $J(R)=P$. 一个局部环的例子是 $R=\{a/b \in \mathbb{Q} : b \text{ 是奇数}\}$，它的唯一极大理想是

$$(2) = \{2a/b : b \text{ 是奇数}\}.$$

例 8.30　设 k 是域，$R=\mathrm{Mat}_n(k)$．对 1 和 n 之间的任意 ℓ，令 $\mathrm{COL}(\ell)$ 表示第 ℓ 列，即

$$\mathrm{COL}(\ell) = \{A=[a_{ij}] \in \mathrm{Mat}_n(k) : \text{对一切 } j \neq \ell, a_{ij}=0\}.$$

易知 $\mathrm{COL}(\ell)=RE_{\ell\ell}$，其中 $E_{\ell\ell}$ 是 $\ell\ell$ 处的元素为 1 而其他元素为 0 的矩阵．我们断言 $\mathrm{COL}(\ell)$ 是 R 中的极小左理想．如果定义

$$\mathrm{COL}^*(\ell) = \sum_{i \neq \ell} \mathrm{COL}(i),$$

则 $\mathrm{COL}^*(\ell)$ 是左理想，且

$$R/\mathrm{COL}^*(\ell) \cong \mathrm{COL}(\ell)$$

是左 R-模．因 $\mathrm{COL}(\ell)$ 是极小左理想，它是单左 R-模，从而 $\mathrm{COL}^*(\ell)$ 是极大左理想．所以，

$$J(R) \subseteq \bigcap_{\ell} \mathrm{COL}^*(\ell) = \{0\},$$

因此 $R=\mathrm{Mat}_n(k)$ 是雅各布森半单的．■

命题 8.31　给定环 R，对 $x \in R$ 下列条件等价：

（ⅰ）$x \in J(R)$；

(ⅱ) 对每个 $r\in R$，元素 $1-rx$ 有左逆，即存在 $u\in R$ 使得 $u(1-rx)=1$；

544 (ⅲ) 对每个极大左理想 I，$x(R/I)=\{0\}$（等价地，对每个单左 R-模 M，$xM=\{0\}$）.

证明　(ⅰ) ⇒ (ⅱ). 如果存在 $r\in R$ 使得 $1-rx$ 没有左逆，则 $R(1-rx)$ 不包含 1，因而是真左理想. 因定理 6.46（每个真理想包含于某个极大理想中）的证明没有用到交换性，所以存在极大左理想 I 使得 $1-rx\in R(1-rx)\subseteq I$. 现在因 $J(R)$ 是左理想，因此 $rx\in J(R)\subseteq I$，从而 $1=(1-rx)+rx\in I$，产生矛盾.

(ⅱ)⇒(ⅲ). 本章前面定义单左 R-模时我们提到一个左 R-模 M 是单的当且仅当 $M\cong R/I$，其中 I 是极大左理想.

假设存在单模 M 满足 $xM\neq\{0\}$；因此存在 $m\in M$ 使得 $xm\neq 0$（当然，$m\neq 0$）. 由此子模 Rxm 包含 $1xm$，从而 $Rxm\neq\{0\}$. 因 M 是单的，它只有一个非零子模，就是 M 自身，从而 $Rxm=M$. 所以存在 $r\in R$ 使得 $rxm=m$，即 $(1-rx)m=0$. 根据假设，$1-rx$ 有左逆，比如 $u(1-rx)=1$. 因此 $0=u(1-rx)m=m$，产生矛盾.

(ⅲ) ⇒ (ⅰ). 如果 $x(R/I)=\{0\}$，则 $x(1+I)=x+I=I$，即 $x\in I$. 所以，如果对每个极大左理想 I 有 $x(R/I)=\{0\}$，则 $x\in\bigcap_I I=J(R)$. ■

注意命题 8.31 中的条件（ⅱ）可以重述为：$x\in J(R)$ 当且仅当对每个 $z\in Rx$，$1-z$ 有左逆.

下面的结果在交换代数中经常用到.

系 8.32 (Nakayama 引理)　如果 M 是有限生成左 R-模，$JM=M$，其中 $J=J(R)$ 是雅各布森根，则 $M=\{0\}$.

特别地，如果 R 是局部环，即 R 是有唯一极大理想 P 的交换环，且 M 是有限生成 R-模满足 $PM=M$，则 $M=\{0\}$.

证明　设 $m_1,\cdots,m_n$ 是 M 的生成集，且在如下的意义下极小：没有它的真子集能够生成 M. 因 $JM=M$，有 $m_1=\sum_{i=1}^{n}r_im_i$，其中 $r_i\in J$. 由此

$$(1-r_1)m_1=\sum_{i=2}^{n}r_im_i.$$

因 $r_1\in J$，命题 8.31 说 $1-r_1$ 有左逆，比如 u，从而 $m_1=\sum_{i=2}^{n}ur_im_i$. 这是一个矛盾，因为现在 M 能被真子集 $\{m_1,\cdots,m_n\}$ 生成.

第二个陈述立刻可得，因为当 R 是有极大理想 P 的局部环时，$J(R)=P$. ■

注　Nakayama 引理中模 M 是有限生成的假设是必要的，例如，容易验证 $R=\{a/b\in\mathbb{Q}:$

545 b 是奇数$\}$ 是有极大理想 $P=(2)$ 的局部环，而 $\mathbb{Q}$ 是一个 R-模，且有 $P\mathbb{Q}=2\mathbb{Q}=\mathbb{Q}$.

注　$J(R)$ 还有其他的刻画. 其中的一个在命题 8.36 中给出，运用 R 中的单位（有左右逆的元素）表示. 还有一个刻画运用左拟正则元素表示：元素 $x\in R$ 称为**左拟正则**的，如果存在 $y\in R$ 使得 $y\circ x=0$（这里 $y\circ x=x+y-yx$ 是圈运算），一个左理想称为**左拟正则**的，如果它的每个元素都是左拟正则的. 可以证明 $J(R)$ 是 R 中唯一的极大左拟正则理想（见 Lam 所著的《A First Course in Noncommutative Rings》67～68 页）.

下一个理想的性质与雅各布森根有关.

定义　称环 R 中的一个左理想 A 为**幂零**的，如果存在某个整数 $m\geqslant 1$ 使得 $A^m=\{0\}$.

回忆 A^m 是形如 $a_1\cdots a_m$ 的积的一切和的集合，其中对一切 $j, a_j \in A$，即 $A^m = \left\{ \sum_i a_{i1}\cdots a_{im} : a_{ij} \in A \right\}$. 由此，如果 A 是幂零的，则每个 $a\in A$ 都是幂零的，即 $a^m = 0$. 另一方面，如果 $a\in R$ 是幂零元素，不能推出由 a 生成的左理想 Ra 是幂零的. 例如 $R = \mathrm{Mat}_2(k)$，其中 k 是某个交换环，令 $a=\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}$. 现在 $a^2=\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$，但 Ra 包含

$$e = \begin{bmatrix}0 & 0\\ 1 & 0\end{bmatrix}\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix} = \begin{bmatrix}0 & 0\\ 0 & 1\end{bmatrix},$$

这是一个幂等元 $e^2=e$. 所以对一切 m，$e^m=e\neq 0$，因此 $(Re)^m \neq \{0\}$.

系 8.33　*设 R 是环，则对 R 中的每个幂零左理想 I 有 $I\subseteq J(R)$.*

证明　设 $I^n = \{0\}$，$x\in I$. 对每个 $r\in R$ 有 $rx\in I$，从而 $(rx)^n=0$. 等式

$$(1+rx+(rx)^2+\cdots+(rx)^{n-1})(1-rx) = 1$$

表明 $1-rx$ 是左可逆的，从而根据命题 8.31，$x\in J(R)$. ■

命题 8.34　*设 R 是左阿廷环，则 $J(R)$ 是幂零理想.*

证明　在这个证明中记 $J(R)$ 为 J. 因 R 是左阿廷环，左理想的降链

$$J\supseteq J^2\supseteq J^3\supseteq\cdots$$

有终止，比如 $J^m = J^{m+1} = \cdots$，记 $I = J^m$，从而 $I = I^2$. 我们假定 $I\neq\{0\}$ 并导致矛盾.

设 $\mathcal{F}$ 是满足 $IB\neq\{0\}$ 的一切非零左理想 B 的族. 因，$I\in\mathcal{F}$，所以 $\mathcal{F}\neq\varnothing$. 根据命题 8.16，存在极小元素 $B_0\in\mathcal{F}$. 选取 $b\in B_0$ 使得 $Ib\neq\{0\}$. 现在

$$I(Ib) = I^2b = Ib\neq\{0\},$$

从而 $Ib\subseteq B_0\in\mathcal{F}$，极小性给出 $B_0 = Ib$. 因 $b\in B_0$，存在 $x\in I\subseteq J = J(R)$ 使得 $b = xb$. 因此 $0 = (1-x)b$. 但根据命题 8.31，$1-x$ 有左逆，比如 u，因此 $0 = u(1-x)b = b$，产生矛盾. ■　[546]

显然雅各布森根是左理想，但它也是右理想；即 $J(R)$ 是双边理想. 我们先给出形成双边理想的另一个来源.

定义　*如果 R 是环，M 是左 R-模，定义 M 的***零化子***为*

$$\mathrm{ann}(M) = \{a\in R : 对一切\ m\in M, am = 0\}.$$

虽然容易看出 $\mathrm{ann}(M)$ 是 R 中的双边理想，我们还是来证明它是右理想. 设 $a\in\mathrm{ann}(M), r\in R$ 和 $m\in M$. 因 M 是左 R-模，有 $rm\in M$. 因 a 零化 M 的每个元素，有 $a(rm) = 0$. 最后，结合性给出对一切 $m, (ar)m = 0$，因此 $ar\in\mathrm{ann}(M)$.

系 8.35　*(i) $J(R) = \bigcap_{I=极大左理想}\mathrm{ann}(R/I)$，从而 $J(R)$ 是 R 中的双边理想.*

(ii) $R/J(R)$ 是雅各布森半单环.

证明　(i)[⊖] 用 $A(R)$ 记 $\bigcap_I\mathrm{ann}(R/I)$，其中对一切极大左理想 I 作交. 对任一左理想 I，

⊖ (i) 的证明是正确的，但下列证明更好：

如果 $x\in J(R)$，则根据命题 8.31，对每一个单左 R-模 M 有 $xM = \{0\}$. 但对某个极大左理想 I 有 $M\cong R/I$；即，$x\in\mathrm{ann}(R/I)$. 于是，$x\in\bigcap_{I=极大左理想}\mathrm{ann}\ (R/I)$.

关于反包含，如果 $x\in\bigcap_{I=极大左理想}\mathrm{ann}\ (R/I)$，则对某个极大左理想 I 的每一个形如 R/I 的左 R-模，有 $xM = \{0\}$. 但每一个单左 R-模 M 都有这种形式，因此 $x\in J(R)$.

我们断言 $\operatorname{ann}(R/I) \subseteq I$．如果 $a \in \operatorname{ann}(R/I)$，则对一切 $r\in R$，有 $a(r+I)=ar+I=I$；即 $ar\in I$. 特别地，如果 $r=1$，则 $a\in I$. 因此 $A(R)\subseteq J(R)$．

关于反包含，假定 I 是一个极大左理想，定义 $S=R/I$，I 的极大性蕴涵 S 是单 R-模．对每个非零 $x\in S$，定义 $\varphi_x: R\to S$ 为 $\varphi_x: r\mapsto rx$．容易验证 φ_x 是 R-映射，因 S 是单的，所以它还是一个满射．于是，$R/\ker\varphi_x \cong S$，且 S 的单性表明左理想 $\ker\varphi_x$ 是极大的．但易知 $\operatorname{ann}(R/I)=\bigcap_{x\in S}\ker\varphi_x$. 由此 $J(R)\subseteq A(R)$．因 $J(R)$等于 $A(R)$，而 $A(R)$是双边理想的交，所以 $J(R)$是双边理想．

（ii）首先，因 $J(R)$是双边理想，所以 $R/J(R)$是环．环的对应定理表明，如果 I 是 R 的包含在 $J(R)$中的双边理想，则 $J(R/I)=J(R)/I$，如果 $I=J(R)$便可得结果． ■

现在我们证明可以用右理想代替左理想来定义雅各布森根．

定义 环 R 中的单位是指有左右逆的元素 $u\in R$，即存在 $v\in R$ 使得

$$uv = 1 = vu.$$

命题 8.36 （i）如果 R 是环，则

547

$$J(R) = \{x \in R: \text{对一切 } r,s \in R, 1+rxs \text{ 是 } R \text{ 中的单位}\}.$$

（ii）如果 R 是环，且 $J'(R)$是 R 的一切极大右理想的交，则 $J'(R)=J(R)$.

证明 （i）令 W 是使得对一切 $r,s\in R$ 有$1+rxs$ 是单位的一切 $x\in R$ 的集合. 如果 $x\in W$，则令 $s=-1$ 得到对一切 $r\in R$，$1-rx$ 是单位．因此 $1-rx$ 有左逆，从而根据命题8.31，$x\in J(R)$. 所以，$W\subseteq J(R)$. 关于反包含，设 $x\in J(R)$. 根据系 8.35，$J(R)$是双边理想，因此对一切 $s\in R$ 有 $xs\in J(R)$. 命题 8.31 说，对一切 $r\in R$，$1-rxs$ 是左可逆的，即存在 $u\in R$ 使得 $u(1-rxs)=1$. 于是，$u=1+urxs$．现在因 $J(R)$是双边理想，所以 $(-ur)xs\in J(R)$，因此 u 有左逆（命题 8.31）．另一方面，u 也有右逆，就是 $1-rxs$. 根据习题 8.16，u 是 R 中的单位．所以对一切 $r,s\in R$, $1-rxs$ 是 R 中的单位．最后，把 r 换成 $-r$，得 $1+rxs$ 是单位，因此 $J(R)\subseteq W$.

（ii）在（i）中对 $J(R)$的描述是左右对称的．在证明命题 8.31 和系 8.35 的右边版本之后，可知 $J'(R)$ 也能如（i）那样描述，从而推出 $J'(R)=J(R)$. ■

习题

8.23 （i）推广引理 6.69 的证明，以此证明如果 Δ 是除环，则由 $\alpha\in\langle S\rangle$ 定义的 $\alpha\preceq S$ 是一个相关关系．

（ii）用定理 6.71 证明除环上的每个左向量空间有基．

（iii）用定理 6.72 证明除环上的一个左向量空间的任意两个基有相同的基数．

8.24 如果 k 是域，A 是有限维 k-代数，定义

$$L = \{\lambda_a \in \operatorname{End}_k(A): \lambda_a: x\mapsto ax\}$$

和

$$R = \{\rho_a \in \operatorname{End}_k(A): \rho_a: x\mapsto xa\}.$$

证明存在 k-代数同构

$$L\cong A \text{ 和 } R\cong A^{op}.$$

提示：证明由 $a\mapsto\lambda_a$ 定义的函数 $A\to L$ 是单射 k-代数映射，因 A 是有限维的，所以它也是满射．

8.25 （i）设 C 是除环 D 的子除环．证明 D 是 C 上的左向量空间，由此可定义 $[D:C]=\dim_C(D)$．

（ii）如果 $Z\subseteq C\subseteq D$ 是除环的塔，其中$[D:C]$和$[C:Z]$有限，则 $[D:Z]$ 有限，且

$$[D : Z] = [D : C][C : Z].$$

提示：如果 $u_1, \cdots, u_m$ 是 D 的作为 C 上的左向量空间的基，$c_1, \cdots, c_d$ 是 C 的作为 Z 上的左向量空间的基，证明一切 $c_i u_j$（在这个次序下）的集合是 D 在 Z 上的基．

548

8.26 （**模律**）设 A，B 和 A' 都是模 M 的子模．如果 $A' \subseteq A$，证明 $A \cap (B + A') = (A \cap B) + A'$．

8.27 （ⅰ）设 $0 \to A \to B \to C \to 0$ 是某个环 R 上的左 R-模的正合列．证明：如果 A，C 都有 DCC，则 B 也有 DCC. 由此推出，此时 $A \oplus B$ 有 DCC.

（ⅱ）设 $0 \to A \to B \to C \to 0$ 是某个环 R 上的左 R-模的正合列．证明：如果 A，C 都有 ACC，则 B 也有 ACC. 由此推出，此时 $A \oplus B$ 有 ACC.

（ⅲ）证明每个成为极小左理想的直和的环都是左阿廷环．

8.28 （L. Small）证明形如 $\begin{bmatrix} a & 0 \\ b & c \end{bmatrix}$ 的一切矩阵的环是左诺特环，但不是右诺特环，其中 $a \in \mathbb{Z}, b, c \in \mathbb{Q}$．

8.29 设 R 是一切 2×2 矩阵 $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ 的环，其中 $a \in \mathbb{Q}, b, c \in \mathbb{R}$．证明 R 是右阿廷环，但不是左阿廷环．

提示：R 中只有有限个右理想，但对 $\mathbb{Q}$ 上的每个向量空间 $V \subseteq \mathbb{R}$，

$$\begin{bmatrix} 0 & V \\ 0 & 0 \end{bmatrix} = \left\{ \begin{bmatrix} 0 & v \\ 0 & 0 \end{bmatrix} : v \in V \right\}$$

是一个左理想．

8.30 举出一个环 R 的例子，它不同构于 R^{op}.

8.31 （ⅰ）如果 R 是交换环，且 $J(R) = \{0\}$，证明 R 没有幂零元．

（ⅱ）举出一个交换环 R 的例子，它没有幂零元，但 $J(R) \neq \{0\}$.

8.32 设 k 是域，$R = \mathrm{Mat}_2(k)$．证明 $a = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ 是左拟正则的，但主左理想 Ra 不是左拟正则理想．

8.33 （ⅰ）如果 Δ 是除环，证明 $\Delta^\times$ 的有限子群未必是循环群．与定理 3.30 作比较．（阿米苏尔（S. A. Amitsur）发现了除环的乘法群的一切有限子群．）

（ⅱ）如果 Δ 是除环，它的中心是特征 $p > 0$ 的域，证明 $\Delta^\times$ 的每个有限子群 G 都是循环群．

提示：考虑 $\mathbb{F}_p G$，并运用定理 8.23.

8.34 如果 R 是环，M 是左 R-模，证明 $\mathrm{Hom}_R(R, M)$ 是左 R-模，并证明它同构于 M.

提示：如果 $f : R \to M$ 和 $r' \in R$，定义 $r'f : r \mapsto f(rr')$．

8.35 如果 k 是特征 0 的域，则 $\mathrm{End}_k(k[t])$ 包含算子

$$x : f(t) \mapsto \frac{\mathrm{d}}{\mathrm{d}t} f(t) \text{ 和 } y : f(t) \mapsto tf(t).$$

（ⅰ）如果 $A_1(k)$ 是由 x 和 y 生成的 $\mathrm{End}_k(k[t])$ 的子代数，证明

$$yx = xy + 1.$$

（ⅱ）证明 $A_1(k)$ 是左诺特环，它没有真非平凡双边理想满足左右消去律（如果 $a \neq 0$，则等式 $ab = ac$ 或等式 $ba = ca$ 蕴涵 $b = c$）．

549

注：习题 8.35 可以这样推广：用 $k[t_1, \cdots, t_n]$ 替代 $k[t]$，用偏导数

$$x_i : f(t_1, \cdots, t_n) \mapsto \frac{\mathrm{d}}{\mathrm{d}t_i} f(t_1, \cdots, t_n)$$

替代算子 x，用

$$y_i : f(t_1, \cdots, t_n) \mapsto t_i f(t_1, \cdots, t_n)$$

替代算子 y. 由 $x_1, \cdots, x_n, y_1, \cdots, y_n$ 生成的 $\mathrm{End}_k(k[t_1, \cdots, t_n])$ 的子代数 $A_n(k)$ 叫做 k 上的 n 次外尔代数.

外尔（H. Weyl）把这个代数引入量子力学中的动量模型和位置算子．可以证明对一切 $n\geqslant 1, A_n(K)$ 是左诺特单整环（见 McConnell-Robson 所著的《Noncommutative Noetherian Rings》19 页）． ■

8.3 半单环

群是一个抽象的对象；我们只能把它画作一个“朦胧之物”，写作一个大写的 G. 当然，存在熟悉的具体的群，诸如对称群 S_n 和域 k 上向量空间 V 的一切非奇异线性变换的一般线性群 $\mathrm{GL}(V)$．有限群 G 的表示是 G 到这种熟悉的群之中的同态，对于 G 它们具有根本上的重要性．

我们先呈示群表示和群环之间的联系．

定义 群 G 的一个 k-表示是一个同态

$$\sigma: G\to \mathrm{GL}(V),$$

其中 V 是域 k 上的向量空间．

注意，如果 $\dim(V)=n$，则 $\mathrm{GL}(V)$ 包含 S_n 的同构复制［如果 $v_1,\cdots,v_n$ 是 V 的一个基且 $\alpha\in S_n$，则存在非奇异线性变换 $T: V\to V$ 使得对一切 $i, T(v_i)=v_{\alpha(i)}$］，所以，置换表示是 k-表示的一种特殊情形．群表示可以翻译为 kG-模的语言（把下面的证明与命题 8.8 作比较）.

命题 8.37 每个 k-表示 $\sigma: G\to\mathrm{GL}(V)$ 把 V 配置成一个左 kG-模的结构，记这个模为 V^σ. 反之，每个左 kG-模 V 确定了一个 k-表示 $\sigma: G\to\mathrm{GL}(V)$.

证明 给定同态 $\sigma: G\to\mathrm{GL}(V)$，记 $\sigma(g): V\to V$ 为 σ_g，并定义作用 $kG\times V\to V$ 为

$$\Big(\sum_{g\in G}a_g g\Big)v=\sum_{g\in G}a_g\sigma_g(v).$$

经简单计算可证明 V 配置了这个标量乘法后是一个左 kG-模．

反之，假定 V 是左 kG-模．如果 $g\in G$，则 $v\mapsto gv$ 定义了一个线性变换 $T_g: V\to V$．此外，T_g 的逆是 T_g^{-1}，所以 T_g 是非奇异的．容易验证由 $\sigma: g\mapsto T_g$ 给出的函数 $\sigma: G\to\mathrm{GL}(V)$ 是 k-表示． ■

550

如果 $\tau: G\to\mathrm{GL}(V)$ 是另一个 k-表示，V^τ 和 V^σ 分别是命题 8.37 中由 τ，σ 确定的 kG-模，那么什么时候 $V^\tau\cong V^\sigma$？回忆如果 $T: V\to V$ 是线性变换，则可以把 V 做成 $k[x]$-模，记为 V^T，并在命题 7.3 中我们知道，如果 $S: V\to V$ 是另一个线性变换，则 $V^S\cong V^T$ 当且仅当存在非奇异 $\varphi: V\to V$ 使得 $S=\varphi T\varphi^{-1}$．

命题 8.38 设 G 是群，$\sigma,\tau: G\to\mathrm{GL}(V)$ 是 k-表示，其中 k 是域．如果 V^σ 和 V^τ 是命题 8.37 中定义的相应的 kG-模，则作为 kG-模有 $V^\sigma\cong V^\tau$ 当且仅当存在非奇异 $\varphi: V\to V$ 使得对每个 $g\in G$,

$$\varphi\tau(g)=\sigma(g)\varphi.$$

注 我们常说 φ **交结** σ 和 τ.

证明 如果 $\varphi: V^\tau\to V^\sigma$ 是 kG-同构，则 $\varphi: V\to V$ 是向量空间的同构，满足对一切 $v\in V$ 和 $g\in G$ 有

$$\varphi\big(\textstyle\sum a_g gv\big)=\big(\textstyle\sum a_g g\big)\varphi(v),$$

但 V^τ 中标量乘法的定义是 $gv=\tau(g)(v)$，而 V^σ 中标量乘法的定义是 $gv=\sigma(g)(v)$．因此对一切 $g\in G$ 和 $v\in V$，有 $\varphi(\tau(g)(v))=\sigma(g)(\varphi(v))$．所以对一切 $g\in G$,

$$\varphi\tau(g)=\sigma(g)\varphi.$$

反之，命题假设给出对一切 $g\in G, \varphi\tau(g)=\sigma(g)\varphi$，其中 φ 是非奇异 k-线性变换，从而对一切 $g\in G$ 和 $v\in V$ 有 $\varphi(\tau(g)v)=\sigma(g)\varphi(v)$．由此易知 φ 是 kG-同构；即 φ 由 $\sum_{g\in G}a_g g$ 保持标量乘法. ■

我们现在用矩阵重述上面的命题．

系 8.39 设 G 是群，$\sigma,\tau: G\to \mathrm{Mat}_n(k)$ 是 k-表示，则作为 kG-模有 $(k^n)^\sigma \cong (k^n)^\tau$ 当且仅当存在非奇异 $n\times n$ 矩阵 P 使得对一切 $x\in G$，

$$P\tau(x)P^{-1} = \sigma(x).$$

例 8.40 如果 G 是有限群，V 是域 k 上的向量空间，则**平凡同态** $\sigma: G\to \mathrm{GL}(V)$ 定义为对一切 $x\in G, \sigma(x)=1_V$．对应的 kG-模 V^σ 叫做**平凡 kG-模**：如果 $v\in V$，则对一切 $x\in G, xv=v$．平凡模 k（也叫做**主 kG-模**）记为 [551]

$$V_0(k).$$

■

现在介绍一个重要的环类；我们将会看到大多数群代数 kG 都是半单环．

定义 称左 R-模是**半单的**，如果它是单模的直和．称环 R 是**左半单的**，如果它是极小左理想的直和[⊖]．

回忆如果把环 R 看作左 R-模，则它的子模是它的左理想，此外，左理想是极小的当且仅当它是单左 R-模．

下一命题推广了例 8.30．

命题 8.41 如果环 R 是左半单的，则它的左理想有两个链条件．

证明 因 R 是左半单的，它是极小左理想的直和：$R=\sum_i L_i$．设 $1=\sum_i e_i$，其中 $e_i\in L_i$．如果 $r=\sum_i r_i\in\sum_i L_i$，则 $r=1r$，从而 $r_i=e_ir_i$．因此，如果 $e_i=0$，则 $L_i=0$．由此可知，只有有限个非零 L_i，即 $R=L_1\oplus\cdots\oplus L_n$．现在列

$$R=L_1\oplus\cdots\oplus L_n\supseteq L_2\oplus\cdots\oplus L_n\supseteq\cdots\supseteq L_n\supseteq\{0\}$$

是合成列，这是因为因子模是 L_1，…，L_n，它们是单的．根据命题 8.17，R（作为它自身上的左 R-模）有两个链条件． ■

我们现在刻画任意环上的半单模．

命题 8.42 一个左模 M（在任意环上）是半单的当且仅当 M 的每个子模都是直和项．

证明 假设 M 是半单的，因此 $M=\sum_{j\in J}S_j$，其中每个 S_j 都是单的．对任意子集 $I\subseteq J$ 定义

$$S_I=\sum_{j\in I}S_j.$$

如果 B 是 M 的子模，佐恩引理给出满足性质 $S_K\cap B=\{0\}$ 的极大子集 $K\subseteq J$，我们断言 $M=B\oplus S_K$．只需证明 $M=B+S_K$，这是因为根据假设它们的交为 $\{0\}$，从而只需证明对一切 $j\in J, S_j\subseteq B+S_K$．如果 $j\in K$，则 $S_j\subseteq S_K\subseteq B+S_K$．如果 $j\notin K$，则极大性给出 $(S_K+S_j)\cap B\neq\{0\}$．于是 [552]

$$s_K+s_j=b\neq 0,$$

其中 $s_K\in S_K, s_j\in S_j, b\in B$．注意 $s_j\neq 0$，否则 $s_K=b\in S_K\cap B=\{0\}$．因此

$$s_j=b-s_K\in S_j\cap(B+S_K),$$

从而 $S_j\cap(B+S_K)\neq\{0\}$．但 S_j 是单的，因此 $S_j=S_j\cap(B+S_K)$，且正如所要的 $S_j\subseteq B+S_K$．所以 $M=B\oplus S_K$．

现在假定 M 的每个子模都是直和项．

⊖ 可以定义一个环是右半单的，如果它是极小右理想的直和．然而，在系 8.57 中，我们将看到一个环是左半单的当且仅当它是右半单的．

（i）每个非零子模 B 包含一个单直和项．

设 $b\in B$ 非零．根据佐恩引理，存在 B 的满足 $b\notin C$ 的极大子模 C. 根据系 7.18，C 是 B 的直和项：存在某个子模 D 使得 $B=C\oplus D$．我们断言 D 是单的．如果 D 不是单的，可以重复刚才的论证证明 $D=D'\oplus D''$，其中 D',D'' 都是非零子模．于是

$$B=C\oplus D=C\oplus D'\oplus D''.$$

我们断言 $C\oplus D'$ 和 $C\oplus D''$ 之中至少一个不包含原先的元素 b. 否则，$b=c'+d'=c''+d''$，其中 c'，$c''\in C,d'\in D'$ 和 $d''\in D''$. 但 $c'-c''=d''-d'\in C\cap D=\{0\}$ 给出 $d'=d''\in D'\cap D''=\{0\}$．因此 $d'=d''=0$，从而 $b=c'\in C$，与 C 的定义矛盾．最后，$C\oplus D'$ 或 $C\oplus D''$ 与 C 的极大性矛盾．

（ii）M 是左半单的．

根据佐恩引理，存在 M 的极大单子模族 $\{S_j:j\in j\}$，使得由这个族中的单子模生成的子模 U 是它们的直和：$U=\sum_{j\in J}S_j$．根据假设，U 是直和项：有某个 M 的子模 V 使得 $M=U\oplus V$．如果 $V=\{0\}$，证明已经完成．否则，根据（i），存在某个包含在 V 中的单子模 S，它是一个直和项：有某个 $V'\subseteq V$ 使得 $V=S\oplus V'$．族 $\{S_j:j\in J\}\cup\{S\}$ 违反了第一个单子模族的极大性，因为这个大族也生成它的直和．所以 $V=\{0\}$，从而 M 是左半单的． ■

系 8.43 （i）一个半单模 M 的每个子模和每个商模都是左半单的．

（ii）如果 R 是（左）半单环，则每个左 R-模都是半单模．

553

（iii）如果 I 是半单环 R 中的双边理想，则商环 R/I 也是半单环．

证明 （i）设 B 是 M 的子模．B 的每个子模 C 自然都是 M 的子模．因 M 是左半单的，所以 C 是 M 的直和项，从而根据系 7.18，C 是 B 的直和项．因此根据命题 8.42，B 是左半单的．

设 M/H 是 M 的商模．现在 H 是 M 的直和项，从而有 M 的某个子模 H' 使得 $M=H\oplus H'$．但根据第一段，H' 是左半单的，且 $M/H\cong H'$．

（ii）存在自由左 R-模 F 和满射 R-映射 $\varphi:F\to M$．现在 R 是它自身上的半单模（这是半单环的定义），因此 F 是一个半单模．于是 M 是半单模 F 的商，从而根据（i）它是半单的．

（iii）首先，因为 I 是双边理想，所以 R/I 是环．根据（i），左 R-模 R/I 是半单的，因此它是直和 $R/I\cong\sum S_j$，其中 S_j 是单左 R-模．但每个 S_j 作为左 (R/I)-模也是单的，这是因为 S_j 的任一 (R/I)-子模也是 S_j 的 R-子模．所以 R/I 是半单的． ■

系 8.44 （i）有限生成左半单 R-模 M（在任意环上）是有限个单左模的直和．特别地，左半单环 R 是有限个极小左理想的直和．

（ii）左半单环 $R_1,\cdots,R_m$ 的直积 $R=R_1\times\cdots\times R_m$ 也是左半单环．

证明 （i）设 $x_1,\cdots,x_n$ 是 M 的生成集．因 M 是左半单的，它是单左模的直和，比如 $M=\sum_j S_j$．现在每个 $x_i=\sum_j s_{ij}$ 只有有限个非零分量，其中 $s_{ij}\in S_j$，因此 $\{x_1,\cdots,x_n\}$ 只涉及有限个 S_j，比如 $S_{j_1},\cdots,S_{j_t}$．所以

$$M\subseteq\langle x_1,\cdots,x_n\rangle\subseteq S_{j_1}\oplus\cdots\oplus S_{j_t}\subseteq M.$$

R 作为自身上的左半单模是循环的，因此是有限生成的．所以 R 仅仅是有限个单左子模的直和；即 R 是有限个极小左理想的直和．

（ii）因每个 R_i 是左半单的，所以它是极小左理想的直和，比如 $R_i=J_{i1}\oplus\cdots\oplus J_{it(i)}$．在例 8.5 中我们看到每个 J_{ik} 不仅是 R_i 中的左理想而且也是 R 中的左理想，由此 J_{ik} 是 R 中的极小左理

想．因此 R 是极小左理想的直和，从而它是左半单环． ■

由此，域的有限直积是交换半单环（本节的后面要证明它的逆）．例如，如果 n 是无平方因子的整数，则孙子剩余定理蕴涵$\mathbb{I}_n$ 是半单环．同样，如果 k 是域，且 $f(x) \in k[x]$ 是不同的不可约多项式的积，则 $k[x]/(f(x))$ 是半单环．

554

我们现在可以推广命题 8.20：除环 Δ 上的每个左向量空间（不必有限生成）都有基．每个除环都是左半单环，Δ 自身是唯一的极小左理想．所以每个左 Δ-模 M 是 Δ 的复制的直和，比如 $M=\sum_{i\in I}\Delta_i$．如果 $x_i \in \Delta_i$ 非零，则 $X=\{x_i : i\in I\}$是 M 的基．这就解释了在命题 8.42 的证明中为什么出现佐恩引理．

下一结果表明左半单环可以用雅各布森根来刻画．

定理 8.45　*环 R 是左半单的当且仅当它是左阿廷环且 $J(R)=\{0\}$.*

证明　如果 R 是左半单的，则根据命题 8.42，存在左理想 I 使得 $R=J(R)\oplus I$．由此根据习题 8.15（ii），存在幂等元 $e\in J(R)$ 和 $f\in I$ 使得 $1=e+f$．因 $e\in J(R)$，命题 8.31 说 $f=1-e$ 有左逆，存在 $u\in R$ 使得 $uf=1$. 但 f 是幂等元，从而 $f=f^2$. 因此 $1=uf=uf^2=(uf)f=f$，从而$e=1-f=0$. 根据习题 8.15（ii），$J(R)e=J(R)$，所以 $J(R)=\{0\}$. 最后，命题 8.41 证明 R 是左阿廷环．

反之，假定 R 是左阿廷环且 $J(R)=\{0\}$. 我们先证明：如果 I 是 R 的极小左理想，则 I 是 R 的直和项．现在 $I\neq\{0\}$，从而 $I\not\subseteq J(R)$；所以存在不包含 I 的极大左理想 A. 因 I 是极小的，所以它是单的，从而 $I\cap A$ 不是 I 就是$\{0\}$. 但 $I\cap A=I$ 蕴涵 $I\subseteq A$，产生矛盾，因此 $I\cap A=\{0\}$. A 的极大性给出 $I+A=R$，所以 $R=I\oplus A$.

选取一个极小左理想 I_1，因 R 是左阿廷环，所以存在这样的极小左理想．正如刚才看到的，有某个左理想 B_1 使得 $R=I_1\oplus B_1$. 现在根据命题 8.29（ii），B_1 包含一个极小左理想，比如 I_2，从而存在左理想 B_2 使得 $B_1=I_2\oplus B_2$. 这个构造法可以迭代，只要 $B_r\neq\{0\}$，就有左理想的严格降链 $B_1\supsetneq B_2\supsetneq\cdots\supsetneq B_{r+1}$. 如果对一切 r，$B_r\neq\{0\}$，则违背 DCC. 所以有某个 r 使得 $B_r=\{0\}$，因此 $R=I_1\oplus\cdots\oplus I_r$ 且 R 是半单的． ■

注意链条件是必需的．例如$\mathbb{Z}$是雅各布森半单的，即 $J(\mathbb{Z})=\{0\}$，但$\mathbb{Z}$不是半单环．

现在我们可以证明下面的值得注意的结果．

定理 8.46（霍普金斯-列维茨基）　*如果环 R 是左阿廷环，则它是左诺特环．*

证明　只要证明 R 作为它自身上的左模有合成列，这样立即可用命题 8.17 证明 R 作为它自身上的模是左诺特环，即 R 有左理想的 ACC.

如果用 $J=J(R)$ 表示雅各布森根，则根据命题 8.34，有某个 $m\geqslant 1$ 使得 $J^m=\{0\}$，从而存在链

$$R=J^0\supseteq J\supseteq J^2\supseteq J^3\supseteq\cdots\supseteq J^m=\{0\}.$$

因每个 J^q 都是R 中的理想，它有 DCC，所以商 J^q/J^{q+1}也有 DCC. 现在根据定理 8.45，R/J 是半单环［它是左阿廷环的商，所以是左阿廷环，根据系 8.35（ii），它是雅各布森半单的］．因子模 J^q/J^{q+1} 是(R/J)-模，因此，根据系 8.43，J^q/J^{q+1} 是半单模，从而它可分解为单(R/J)-模的直和（可能无限）．但只能有有限个直和项，这是因为 J^q/J^{q+1} 的每个(R/J)-子模必定是 R-子模，而 J^q/J^{q+1} 关于 R-子模有 DCC. 因此存在单(R/J)-模 S_i 使得

555

$$J^q/J^{q+1}=S_1\oplus S_2\oplus\cdots\oplus S_p.$$

一次删除一个单直和项产生 J^q/J^{q+1} 的一个列，它的第 i 个因子模是

$$(S_i\oplus S_{i+1}\oplus\cdots\oplus S_p)/(S_{i+1}\oplus\cdots\oplus S_p)\cong S_i.$$

现在单 (R/J)-模 S_i 是被 J 零化的 R-模，所以 S_i 也是一个单 R-模，因此我们已经构造了 J^q/J^{q+1} 作为左 R-模的一个合成列．最后，对每个 q 用这种方法加细 R 原来的列，得到 R 的合成列． ■

当然，定理 8.46 的逆命题不成立．

下一结果是基本的．

定理 8.47 (Maschke 定理) 如果 G 是有限群，k 是特征不能整除 $|G|$ 的域，则 kG 是左半单环．

注 如果 k 有特征 0，假设恒成立．

证明 根据命题 8.42，只要证明 kG 的每个左理想 I 都是直和项．因 k 是域，kG 是 k 上的向量空间，I 是子空间．根据系 6.49，I 是（向量空间的）直和项：存在子空间 V（它可以不是 kG 中的左理想）使得 $kG = I \oplus V$．存在 k-线性变换 $d: kG \to I$ 使得对一切 $b \in I$ 有 $d(b) = b$ 且 $\ker d = V$ [每个 $u \in kG$ 有形如 $u = b + v$ 的唯一表达式，其中 $b \in I$ 和 $v \in V, d(u) = b$]．如果 d 是 kG-映射而不仅是 k-映射，则根据系 7.17 的判别法，证明就可以完成：I 是 kG 的直和项当且仅当它是一个收缩核；即存在 kG-映射 $D: kG \to I$ 使得对一切 $u \in I$ 有 $D(u) = u$．我们现在用一种“平均”方法迫使 d 成为一个 kG-映射．

定义 $D: kG \to kG$ 为对一切 $u \in kG$，

$$D(u) = \frac{1}{|G|}\sum_{x \in G} xd(x^{-1}u).$$

注意根根据对 k 的特征的假设，在 k 中 $|G| \neq 0$，因此它可逆．显然 D 是一个 k-映射．

(i) $\operatorname{im} D \subseteq I$.

如果 $u \in kG$ 和 $x \in G$，则 $d(x^{-1}u) \in I$(因为 $\operatorname{im} d \subseteq I$)，因为 I 是左理想，所以 $xd(x^{-1}u) \in I$. 所以，$D(u)$ 定义中的每个项都在 I 中，从而 $D(u) \in I$.

556

(ii) 如果 $b \in I$，则 $D(b) = b$.

因 $b \in I$，从而 $x^{-1}b \in I$，且 $d(x^{-1}b) = x^{-1}b$. 于是 $xd(x^{-1}b) = xx^{-1}b = b$. 所以 $\sum_{x \in G} xd(x^{-1}b) = |G|b$，因此 $D(b) = b$.

(iii) D 是一个 kG-映射．

只要证明对一切 $g \in G$ 和一切 $u \in kG$ 有 $D(gu) = gD(u)$．而

$$\begin{aligned} gD(u) &= \frac{1}{|G|}\sum_{x \in G} gxd(x^{-1}u) \\ &= \frac{1}{|G|}\sum_{x \in G} gxd(x^{-1}g^{-1}gu) \\ &= \frac{1}{|G|}\sum_{y = gx \in G} yd(y^{-1}gu) \\ &= D(gu) \end{aligned}$$

(因 x 遍历 G，所以 $y = gx$ 也遍历 G)． ■

Maschke 定理的逆定理也成立：如果 G 是有限群，k 是域，它的特征 p 整除 $|G|$，则 kG 不是左半单的，习题 8.37 有一个证明的概要．

进一步分析左半单环之前，我们给出它们的几个特征．

命题 8.48 在环 R 上下列条件等价：

(i) R 是左半单环．

(ii) 每个左 R-模都是半单模．

(iii) 每个左 R-模都是内射模．

（iv）每个左 R-模的短正合列分裂．

（v）每个左 R-模都是投射模．

证明　（i）⇒（ii）．由系 8.43（ii）（如果 R 是半单环，则每个 R-模都是半单模）立得．

（ii）⇒（iii）．如果 E 是左 R-模，则命题 7.64 说，如果每个正合列 $0\to E\to B\to C\to 0$ 分裂，则 E 是内射模．根据假设，B 是半单模，从而命题 8.42 蕴涵序列分裂，即 E 是内射模．

（iii）⇒（iv）．如果 $0\to A\to B\to C\to 0$ 是正合列，则和每个模一样，只要 A 是内射模，该正合列必分裂（见命题 7.64）．

（iv）⇒（v）．给定模M，存在正合列

$$0\to F'\to F\to M\to 0,$$

557

其中 F 是自由的．根据假设，该序列分裂，从而 $F\cong M\oplus F'$. 所以 M 是自由模的直和项，因此它是投射模（见定理 7.56）．

（v）⇒（i）．如果 I 是 R 的左理想，则

$$0\to I\to R\to R/I\to 0$$

是一个正合列．根据假设，R/I 是投射的，所以该序列分裂（见命题 7.54），即 I 是 R 的直和项．根据命题 8.42，R 是左半单 R-模．所以 R 是左半单环．■

由于半单环上的模的优良性质，以致有环 R 的整体维数的概念，用以测量 R 离开半单性程度，我们将在第 11 章中讨论整体维数．

下面是更多左半单环的例子，韦德伯恩-阿廷定理证明再没有其他的左半单环．

命题 8.49　（i）*如果 Δ 是除环，V 是 Δ 上的左向量空间，且 $\dim(V)=n$，则 $\mathrm{End}_\Delta(V)\cong\mathrm{Mat}_n(\Delta^{\mathrm{op}})$ 是左半单环．*

（ii）*如果 $\Delta_1,\cdots,\Delta_m$ 都是除环，则*

$$\mathrm{Mat}_{n_1}(\Delta_1)\times\cdots\times\mathrm{Mat}_{n_m}(\Delta_m)$$

是左半单环．

证明　（i）根据命题 8.24，有

$$\mathrm{End}_\Delta(V)\cong\mathrm{Mat}_n(\mathrm{End}_\Delta(\Delta));$$

根据命题 8.12，$\mathrm{End}_\Delta(\Delta)\cong\Delta^{\mathrm{op}}$．所以 $\mathrm{End}_\Delta(V)\cong\mathrm{Mat}_n(\Delta^{\mathrm{op}})$．

我们证明 $\mathrm{End}_\Delta(V)$ 是半单的．如果 $v_1,\cdots,v_n$ 是 V 的基，定义

$$\mathrm{Col}(j)=\{T\in\mathrm{End}_\Delta(V):\text{对一切 } i\neq j \text{ 有 } T(v_i)=0\}.$$

易知 $\mathrm{Col}(j)$是 $\mathrm{End}_\Delta(V)$ 中的左理想：如果 $S\in\mathrm{End}_\Delta(V)$，则对一切 $i\neq j$ 有 $S(Tv_i)=0$．回忆例 8.30：如果我们考察 $\mathrm{Mat}_n(\Delta^{\mathrm{op}})\cong\mathrm{End}_\Delta(V)$，则 $\mathrm{Col}(j)$对应于 $\mathrm{COL}(j)$，它是除第 j 列外都是 0 的所有矩阵．显然

$$\mathrm{Mat}_n(\Delta^{\mathrm{op}})=\mathrm{COL}(1)\oplus\cdots\oplus\mathrm{COL}(n).$$

因此，$\mathrm{End}_\Delta(V)$ 也是这样的直和．我们断言在例 8.30 中，每个 $\mathrm{COL}(j)$ 都是极小左理想，从而 $\mathrm{End}_\Delta(V)$ 是左半单环．现在我们证明 $\mathrm{Col}(j)$ 的极小性．

假设 I 是 $\mathrm{End}_\Delta(V)$ 中的非零左理想，且 $I\subseteq\mathrm{Col}(j)$．选取非零的 $F\in I$，现在 $F(v_j)=u\neq 0$，否则 F 会消去每个基元素从而变成0. 如果 $T\in\mathrm{Col}(j)$，记 $T(v_j)=w$．因 $u\neq 0$，存在 $S\in\mathrm{End}_\Delta(V)$ 使得 $S(v)=w$．现在

558

$$SF(v_i) = \begin{cases} 0 & \text{如果 } i \neq j \\ S(u) = w & \text{如果 } i = j. \end{cases}$$

所以 $T = SF$，这是因为它们在基上一致．因 I 是左理想，从而 $T \in I$. 所以 $\mathrm{Col}(j) = I$，且 $\mathrm{Col}(j)$ 是极小左理想．

（ⅱ）从（ⅰ）和命题 8.44（ⅱ）立得，因为，如果 Δ 是除环，则根据习题 8.13，Δ^{op} 也是除环．■

系 8.50　*如果 V 是除环 Δ 上的 n 维左向量空间，则对 $1 \leqslant j \leqslant n$, $\mathrm{End}_\Delta(V)$ 中的一切极小左理想 $\mathrm{Col}(j)$ 都同构．*

证明　设 $v_1, \cdots, v_n$ 是 V 的基．对每个 j 定义 $p_j : V \to V$ 为交换 v_j 和 v_1 而固定其他 v_i 的线性变换．易知 $T \mapsto Tp_j$ 是同构 $\mathrm{Col}(1) \to \mathrm{Col}(j)$．■

在引理8.61(ⅱ)中，我们会看到 $\mathrm{End}_\Delta(V)$ 中的一切极小左理想都同构．

定义　*称环 R 为**单环**，如果 R 是非零的且 R 没有非零真双边理想．*

在命题 8.59 中，我们会看到每个左阿廷单环都是半单的．

命题 8.51　*如果 Δ 是除环，则 $R = \mathrm{Mat}_n(\Delta)$ 是单环．*

证明　一个**矩阵单位** E_{pq} 是一个 $n \times n$ 矩阵，该矩阵除 p, q 处的元素为 1 之外，其他元素都是 0. 矩阵单位形成看作 Δ 上左向量空间的 $\mathrm{Mat}_n(\Delta)$ 的基，这是因为每个矩阵 $A = [a_{ij}]$ 有唯一的表达式

$$A = \sum_{ij} a_{ij} E_{ij}.$$

[当然，这就是说 $\dim(\mathrm{Mat}_n(\Delta)) = n^2$.] 经简单计算可知矩阵单位按照下面的法则相乘：

$$E_{ij}E_{k\ell} = \begin{cases} 0 & \text{如果 } j \neq k \\ E_{i\ell} & \text{如果 } j = k. \end{cases}$$

559　假设 N 是 $\mathrm{Mat}_n(\Delta)$ 中的非零双边理想．如果 A 是 N 中的非零矩阵，比如它有非零元素 $a_{ij} \neq 0$. 因 N 是双边理想，对一切 p, q, N 包含 $E_{pi}AE_{jq}$．但

$$\begin{aligned} E_{pi}AE_{jq} &= E_{pi} \sum_{k\ell} a_{k\ell} E_{k\ell} E_{jq} \\ &= E_{pi} \sum_{k} a_{kj} E_{kq} \\ &= \sum_{k} a_{kj} E_{pi} E_{kq} \\ &= a_{ij} E_{pq}. \end{aligned}$$

因 $a_{ij} \neq 0$，且 Δ 是除环，所以 $a_{ij}^{-1} \in \Delta$，从而对一切 $p, q, E_{pq} \in N$. 而一切 E_{pq} 的集合张成 Δ 上的左向量空间 $\mathrm{Mat}_n(\Delta)$，因此 $N = \mathrm{Mat}_n(\Delta)$．■

我们现在证明命题8.49(ⅱ)的逆：每个左半单环都同构于除环上的矩阵环的直积．第一步呈示如何产生除环．

定理 8.52（舒尔引理）　*设 M 和 M' 都是单左 R-模，其中 R 是环．*

（ⅰ）每个非零 R-映射 $f : M \to M'$ 都是一个同构．

（ⅱ）$\mathrm{End}_R(M)$ 是除环．特别地，如果 L 是环 R 中的极小左理想，则 $\mathrm{End}_R(L)$ 是除环．

证明　（ⅰ）因 M 是单的，它只有两个子模：M 自身和 $\{0\}$．现在因为 $f \neq 0$，所以子模 $\ker f \neq M$，从而 $\ker f = \{0\}$，即 f 是单射．同样，子模 $\mathrm{im} f \neq \{0\}$，从而 $\mathrm{im} f = M'$，所以 f 是满射．

（ⅱ）如果 $f : M \to M$ 且 $f \neq 0$，则根据（ⅰ），f 是同构，因此它有逆 $f^{-1} \in \mathrm{End}_R(M)$．于是环 $\mathrm{End}_R(M)$ 是除环．■

引理 8.53 如果 L 和 L' 都是环 R 的极小左理想，则下面每个陈述蕴涵它下面的一个：

(1) $LL' \neq \{0\}$；

(2) $\mathrm{Hom}_R(L,L') \neq \{0\}$ 且存在 $b' \in L'$ 使得 $L' = Lb'$；

(3) 作为左 R-模有 $L \cong L'$.

如果还有 $L^2 \neq \{0\}$，则 (3) 蕴涵 (1)，即三个陈述等价.

证明 设 L 和 L' 都是极小左理想.

(1)⇒(2). 如果 $LL' \neq \{0\}$，则存在 $b \in L$ 和 $b' \in L'$ 使得 $bb' \neq 0$. 于是由 $x \mapsto xb'$ 定义的函数 $f: L \to L'$ 是非零 R-映射，从而 $\mathrm{Hom}_R(L,L') \neq \{0\}$. 此外，因为 Lb' 是极小左理想 L' 的非零子模，所以 $Lb' = L'$.

560

(2)⇒(3). 如果 $\mathrm{Hom}_R(L,L') \neq \{0\}$，则存在非零的 $f: L \to L'$，根据舒尔引理，f 是同构，即 $L \cong L'$.

(3) 和 $L^2 \neq \{0\}$⇒(1). 假定 $L^2 \neq \{0\}$，于是存在 $x,y \in L$ 使得 $xy \neq 0$. 如果 $g: L \to L'$ 是同构，则 $0 \neq g(xy) = xg(y) \in LL'$，因此 $LL' \neq \{0\}$. ■

注意，如果 $J(R) = \{0\}$，则 $L^2 \neq \{0\}$. 否则 L 是幂零左理想，系 8.33 给出 $L \subseteq J(R) = \{0\}$，产生矛盾.

命题 8.54 如果 $R = \sum_j L_j$ 是左半单环，其中 L_j 是极小左理想，则每个单 R-模 S 同构于某个 L_j.

证明 现在根据习题 8.34，$S \cong \mathrm{Hom}_R(R,S) \neq \{0\}$. 如果对一切 j，$\mathrm{Hom}_R(L_j,S) = \{0\}$，则 $\mathrm{Hom}_R(R,S) = \{0\}$（因为 $R = L_1 \oplus \cdots \oplus L_m$）. 因此有某个 j 使得 $\mathrm{Hom}_R(L_j,S) \neq \{0\}$. 因 L_j 和 S 都是单的，定理 8.52（i）给出 $L_j \cong S$. ■

下面是一个富于想象的证明.

证明 根据系 7.14，存在左理想 I 使得 $S \cong R/I$，从而存在列

$$R \supseteq I \supseteq \{0\}.$$

在命题 8.41 中，我们看到

$$R = L_1 \oplus \cdots \oplus L_n \supseteq L_2 \oplus \cdots \oplus L_n \supseteq \cdots \supseteq L_n \supseteq \{0\}$$

是合成列，它的因子模是 $L_1, \cdots, L_n$. 现在施赖埃尔加细定理（定理 8.15）说这两个列有等价的加细. 因一个合成列只允许有重复其项的加细，所以因子模 S 出现在第一个列的加细中必同构于第二个列的一个因子模，即有某个 i 使得 $S \cong L_i$. ■

例 8.55 平凡 kG-模 $V_0(k)$（见例 8.40）是一个单 kG-模（因为它是一维的，除了 $\{0\}$ 和它自身外没有其他的子空间）. 根据命题 8.54，$V_0(k)$ 同构于 kG 的某个极小左理想 L. 我们寻找 kG 中满足对一切 $h \in G$ 有 $hu = u$ 的元素 $u = \sum_{g \in G} a_g g$，以此求出 L. 对于这样的元素 u，

$$hu = \sum_{g \in G} a_g hg = \sum_{g \in G} a_g g = u.$$

因 G 中的元素形成向量空间 kG 的基，所以系数相同，从而对一切 $g \in G$ 有 $a_g = a_{hg}$，特别地，$a_1 = a_h$. 由于该式对每个 $h \in G$ 成立，因此一切系数 a_g 都相等. 所以，如果定义 $\gamma \in kG$ 为

$$\gamma = \sum_{g \in G} g,$$

561

则 u 是 γ 的标量倍. 由此，$L = \langle \gamma \rangle$ 是一个左理想同构于平凡模 $V_0(k)$. 此外，$\langle \gamma \rangle$ 是唯一的这样的左理想. ■

一个抽象的左半单环 R 是极小左理想的直和：$R=\sum_j L_j$，并且我们知道对每个 j，$\mathrm{End}_R(L_j)$ 是除环．下一步是求 R 的直和项，这些直和项最终是矩阵环；它们来自归并同构项得到的 R 的极小左理想分解．

定义 设 R 是左半单环，并设

$$R=L_1\oplus\cdots\oplus L_n,$$

其中 L_j 是极小左理想．给直和项重新标号，使得最先的 m 个理想 L_1，…，L_m 没有两个同构，而在给定的分解中，每个 L_j 同构于某个 L_i，其中 $1\leqslant i\leqslant m$．左理想

$$B_i=\sum_{L_j\cong L_i}L_j$$

称为 R 关于分解 $R=\sum_j L_j$ 的**单分量**．

在系 8.62 中，我们将看到单分量不依赖于 R 的极小左理想的直和分解．

我们把韦德伯恩-阿廷定理[⊖]分为两部分：一个存在定理和一个唯一性定理．

定理 8.56（韦德伯恩-阿廷 I） 环 R 是左半单环当且仅当 R 同构于一个除环上的矩阵环的直积．

证明 充分性是命题 8.49.

关于必要性，假定 R 是左半单的．现在 R 是它的单分量的直和：

$$R=B_1\oplus\cdots\oplus B_m,$$

其中每个 B_i 是同构极小左理想的直和．命题 8.12 说存在环同构

$$R^{\mathrm{op}}\cong\mathrm{End}_R(R),$$

其中 R 看作它自身上的左模．现在根据引理 8.53，对一切 $i\neq j$，$\mathrm{Hom}_R(B_i,B_j)=\{0\}$，从而运用系 8.26 得到环同构

$$R^{\mathrm{op}}\cong\mathrm{End}_R(R)\cong\mathrm{End}_R(B_1)\times\cdots\times\mathrm{End}_R(B_m).$$

因为 B_i 是 L_i 的同构复制的直和，根据命题 8.24，存在环同构

562

$$\mathrm{End}_R(B_i)\cong\mathrm{Mat}_{n_i}(\mathrm{End}_R(L_i)),$$

根据舒尔引理，$\mathrm{End}_R(L_i)$ 是除环，比如 Δ_i，从而

$$R^{\mathrm{op}}\cong\mathrm{Mat}_{n_1}(\Delta_1)\times\cdots\times\mathrm{Mat}_{n_m}(\Delta_m).$$

因此，

$$R\cong[\mathrm{Mat}_{n_1}(\Delta_1)]^{\mathrm{op}}\times\cdots\times[\mathrm{Mat}_{n_m}(\Delta_m)]^{\mathrm{op}}.$$

最后，命题 8.13 给出

$$R\cong\mathrm{Mat}_{n_1}(\Delta_1^{\mathrm{op}})\times\cdots\times\mathrm{Mat}_{n_m}(\Delta_m^{\mathrm{op}}).$$

因为根据习题 8.13，对一切 i，Δ_i^{op} 也是除环，从而证明完成． ■

系 8.57 环 R 是左半单环当且仅当它是右半单环．

证明 易知环 R 是右半单的当且仅当它的对立环 R^{op} 是左半单的．但在定理 8.56 的证明的中间部分，我们看到

$$R^{\mathrm{op}}\cong\mathrm{Mat}_{n_1}(\Delta_1)\times\cdots\times\mathrm{Mat}_{n_m}(\Delta_m),$$

其中 $\Delta_i=\mathrm{End}_R(L_i)$. ■

⊖ 韦德伯恩对半单 k-代数证明了这个定理，其中 k 是域；阿廷把这个定理推广为这里陈述的那样．这个定理说明了阿廷环这个名称的来由．

作为这个系的一个推论，我们可以说一个环是半单的，而不必有形容词左或右．

系 8.58　*交换环 R 是半单的当且仅当它同构于有限个域的直积．*

证明　域是半单环，从而根据系 8.44（ⅱ），有限个域的直积也是半单的．反之，如果 R 是半单的，则它是除环上的矩阵环的直积．因 R 是交换的，所有矩阵环必定都是 1×1 大小的，且所有除环必定都是域．■

虽然半单的名称似乎蕴涵单环是半单的，但这是不清楚的．事实上，没有 DCC 的假定，这是错的（单环不是半单环的例子见 Lam 所著的《A First Course in Noncommutative Rings》，43 页）．

命题 8.59　*单左阿廷环 R 是半单的.*

证明（Janusz）　因 R 是左阿廷环，它包含一个极小左理想，比如 L，当然 L 是单左 R-模．对每个 $a\in R$，由 $f_a(x)=xa$ 定义的函数 $f_a: L\to R$ 是左 R-模映射：如果 $r\in R$，则

$$f_a(rx)=(rx)a=r(xa)=rf_a(x).$$

563

现在 $\operatorname{im} f_a=La$，而 L 是单模迫使 $\ker f_a=L$ 或 $\ker f_a=\{0\}$．在第一种情形有 $La=\{0\}$；在第二种情形有 $L\cong La$．于是，La 或都是$\{0\}$ 或者是一个单模.

考虑和 $I=\left\langle \bigcup_{a\in R} La\right\rangle\subseteq R$．显然，$I$ 是左理想；它也是右理想，这是因为对 $b\in R$ 和 $La\subseteq I$ 有 $(La)b=L(ab)\subseteq I$．因 R 是单环，非零双边理想 I 必等于 R. 我们断言 R 是有限个 La 的和. 如同 R 中的任一元素，幺元 1 在某个 La 的有限和中；比如 $1\in Le_1+\cdots+Le_n$．如果 $b\in R$，则 $b=b1\in b(Le_1+\cdots+Le_n)\subseteq Le_1+\cdots+Le_n$（因为 $Le_1+\cdots+Le_n$ 是左理想）．因此，$R=Le_1+\cdots+Le_n$.

为证明 R 是半单的，只要证明它是单子模的直和．取 n 为满足 $R=Le_1+\cdots+Le_n$ 的极小整数；我们断言 $R=Le_1\oplus\cdots\oplus Le_n$．根据命题 7.19，只要证明对一切 i，

$$Le_i\cap\Big(\sum_{j\neq i}Le_j\Big)=\{0\}.$$

如果这个交不是 $\{0\}$，则 Le_i 的单性表明 $Le_i\cap\Big(\sum_{j\neq i}Le_j\Big)=Le_i$；即 $Le_i\subseteq\sum_{j\neq i}Le_j$，这与选取的 n 是极小的矛盾. 因此，R 是半单环. ■

下面的系由命题 8.59 和韦德伯恩-阿廷定理立得．

系 8.60　*如果 A 是单左阿廷环，则有某个 $n\geqslant 1$ 和某个除环 Δ 使得 $A\cong \mathrm{Mat}_n(\Delta)$.*

下一引理给出左半单环享有的一些重要性质，将用来完成韦德伯恩-阿廷定理，这通过陈述它的组成成员的唯一性来实现．特别地，要证明系 8.60 中的整数 n 和除环 Δ 是由 A 唯一确定．

564

引理 8.61　*设 R 是左半单环，并设*

$$R=L_1\oplus\cdots\oplus L_n=B_1\oplus\cdots\oplus B_m,$$

其中 L_j 是极小左理想，B_i 是 R 相应的单分量．

（ⅰ）每个 B_i 是环，且是 R 中的双边理想，当 $j\neq i$ 时，$B_iB_j=\{0\}$．

（ⅱ）如果 L 是 R 中的任一极小左理想，它不必出现在 R 的给定的分解中，则有某个 i 使得 $L\cong L_i$ 且 $L\subseteq B_i$．

（ⅲ）R 中的每个双边理想 D 是若干 B_i 的直和．

（ⅳ）每个 B_i 都是单环．

证明　（ⅰ）每个 B_i 都是左理想．为证明它也是右理想，考虑

$$B_iR=B_i(B_1\oplus\cdots\oplus B_m)\subseteq B_iB_1+\cdots+B_iB_m.$$

回忆对每个 i，B_i 是同构于 L_i 的若干左理想 L 的直和．如果 $L\cong L_i$ 和 $L'\cong L_j$，则运用引理 8.53 中

的逆否命题非（3）⇒非（1）得到当 $j \neq i$ 时 $LL' = \{0\}$．因此，如果 $j \neq i$，

$$B_iB_j = \Big(\sum_{L \cong L_i} L\Big)\Big(\sum_{L' \cong L_j} L'\Big) \subseteq \sum LL' = \{0\}.$$

于是，$B_iB_1 + \cdots + B_iB_m \subseteq B_iB_i$．因 B_i 是左理想，所以 $B_iB_i \subseteq RB_i \subseteq B_i$．由此 $B_iR \subseteq B_i$，所以 B_i 是右理想，因此它是双边理想．

在证明 B_i 是右理想的最后一步中，我们看到 $B_iB_i \subseteq B_i$，即 B_i 在乘法下封闭．所以要证明 B_i 是环，现在只要证明它包含幺元．如果 1 是 R 中的幺元，则 $1 = e_1 + \cdots + e_m$，其中对一切 i，$e_i \in B_i$．如果 $b_i \in B_i$，则

$$b_i = 1b_i = (e_1 + \cdots + e_m)b_i = e_ib_i,$$

这是因为由（i），只要 $j \neq i$ 就有 $B_jB_i = \{0\}$．同样，等式 $b_i = b_i1$ 给出 $b_ie_i = b_i$，因此 e_i 是 B_i 中的幺元．所以 B_i 是环[⊖]．

（ii）根据命题 8.54，有某个 i 使得极小左理想 L 同构于 L_i．现在

$$L = RL = (B_1 \oplus \cdots \oplus B_m)L \subseteq B_1L + \cdots + B_mL.$$

如果 $j \neq i$，则根据引理 8.53，$B_jL = \{0\}$．因 B_i 是右理想，所以有

565

$$L \subseteq B_iL \subseteq B_i.$$

（iii）R 中的非零双边理想 D 是左理想，根据命题 8.29（ii），它包含某个极小左理想 L．现在根据命题 8.54，有某个 i 使得 $L \cong L_i$，我们断言 $B_i \subseteq D$．根据引理 8.53，如果 L' 是 B_i 中的任一极小左理想，则有某个 $b' \in L'$ 使得 $L' = Lb'$．因 $L \subseteq D$ 且 D 是右理想，我们有 $L' = Lb' \subseteq LL' \subseteq DR \subseteq D$．我们已经证明了 D 包含每个同构于 L_i 的左理想；由于 B_i 是由这种理想生成的，所以 $B_i \subseteq D$．记 $R = B_I \oplus B_J$，其中 $B_I = \sum_i B_i$ 满足 $B_i \subseteq D$，以及 $B_J = \sum_j B_j$ 满足 $B_j \not\subseteq D$．根据系 7.18（它对非交换环上的模成立），$D = B_I \oplus (D \cap B_J)$．但 $D \cap B_J = \{0\}$，否则它要包含某个极小左理想 $L \cong L_j$，其中 $j \in J$，和上面一样，这迫使 $B_j \subseteq D$．所以 $D = B_I$．

（iv）B_i 中的左理想也是 R 中的左理想：如果 $a \in R$，则 $a = \sum_j a_j$，其中 $a_j \in B_j$；如果 $b_i \in B_i$，则因 $j \neq i$ 时 $B_jB_i = \{0\}$，所以有

$$ab_i = (a_1 + \cdots + a_m)b_i = a_ib_i \in B_i.$$

同样，B_i 中的右理想也是 R 中的右理想，因此 B_i 中的双边理想 D 也是 R 中的双边理想．根据（iii），R 中的双边理想都是单分量的直和，因此 $D \subseteq B_i$ 蕴涵 $D = \{0\}$ 或 $D = B_i$，所以 B_i 是单环． ■

系 8.62 如果 R 是半单环，则包含一个极小左理想 L_i 的单分量是由一切同构于 L_i 的极小左理想生成的左理想．所以，半单环的单分量不依赖于 R 的极小左理想的直和分解．

证明 由引理 8.61（ii）可得． ■

系 8.63 （i）如果 A 是单阿廷环，则有某个除环 Δ 使得 $A \cong \mathrm{Mat}_n(\Delta)$．如果 L 是 A 中的极小左理想，则每个单左 A-模同构于 L，此外，$\Delta^{\mathrm{op}} \cong \mathrm{End}_A(L)$．

（ii）两个左 A-模 M 和 N 同构当且仅当 $\dim_\Delta(M) = \dim_\Delta(N)$．特别地，如果 $A = \mathrm{Mat}_m(\Delta)$，则 $M \cong N$ 当且仅当 $\dim_\Delta(M) = \dim_\Delta(N)$．

证明 因 A 是半单环，每个左模 M 同构于一个极小左理想的直和．但根据引理 8.61（ii），一切极小左理想都同构，比如同构于 L，从而 $\dim_\Delta(M)/n$ 是分解中直和项的个数．如果作为左 $\mathrm{Mat}_n(\Delta)$-

⊖ B_i 不是 R 的子环，因为幺元 e_i 不是 R 中的幺元 1.

模$M\cong N$，则作为左Δ-模$M\cong N$，从而$\dim_\Delta(M)=\dim_\Delta(N)$．反之，如果$\dim_\Delta(M)=nd=\dim_\Delta(N)$，则$M$和$N$都是$L$的$d$个复制的直和，因此作为左$A$-模$M\cong N$.

现在可以假定$A=\mathrm{Mat}_n(\Delta)$和$L=\mathrm{Col}(1)$，$\mathrm{Col}(1)$是由后面$n-1$列为0的一切$n\times n$矩阵组成的极小左理想（见命题8.49）．定义$\varphi:\Delta\to\mathrm{End}_A(L)$如下：如果$d\in\Delta$和$\ell\in L$，则$\varphi_d:\ell\mapsto\ell d$.注意$\varphi_d$是$A$-映射：它是加性的且如果$a\in A$和$\ell\in L$则有$\varphi_d(a\ell)=(a\ell)d=a(\ell d)=a\varphi_d(\ell)$．其次，$\varphi$是环反同态：$\varphi_1=1_L$，它是加性的，且$\varphi_{dd'}=\varphi_{d'}\varphi_d$：如果$\ell\in L$，则$\varphi_{d'}\varphi_d(\ell)=\varphi_d(\ell d')=\ell d'd=\varphi_{dd'}(\ell)$；即$\varphi$是环同态$\Delta^{\mathrm{op}}\to\mathrm{End}_A(L)$．为证明$\varphi$是单射，注意每个$\ell\in L\subseteq\mathrm{Mat}_n(\Delta)$是元素在$\Delta$中的矩阵，因此$\ell d=0$蕴涵$\ell=0$．最后证明$\varphi$是满射．设$f\in\mathrm{End}_A(L)$．现在$L=AE_{11}$，其中$E_{11}$是矩阵单位（每个单模由它的任一非零元素生成）．如果$u_i\in\Delta$，令$[u_1,\cdots,u_n]$表示L中第一列是$(u_1,\cdots,u_n)^t$而其他元素都为0的$n\times n$矩阵．记$f(E_{11})=[d_1,\cdots,d_n]$．如果$\ell\in L$，则$\ell$形如$[u_1,\cdots,u_n]$，只要用矩阵乘法的定义容易看出$[u_1,\cdots,u_n]=[u_1,\cdots,u_n]E_{11}$．因$f$是$A$-映射，

$$\begin{aligned}f([u_1,\cdots,u_n])&=f([u_1,\cdots,u_n]E_{11})\\&=[u_1,\cdots,u_n]f(E_{11})\\&=[u_1,\cdots,u_n][d_1,\cdots,d_n]\\&=[u_1,\cdots,u_n]d_1=\varphi_{d_1}([u_1,\cdots,u_n]).\end{aligned}$$

所以正如所要的$f=\varphi_{d_1}\in\mathrm{im}\varphi$. ■

566

R的单分量的个数m是一个不变量，因为它是不同构的单左R-模的个数．然而还有更强的唯一性结果．

定理8.64（韦德伯恩-阿廷II）　*每个半单环R都是一个直积，*

$$R\cong\mathrm{Mat}_{n_1}(\Delta_1)\times\cdots\times\mathrm{Mat}_{n_m}(\Delta_m),$$

其中$n_i\geqslant1$，Δ是除环，并且数m和n_i以及除环Δ_i由R唯一确定．

证明　设R是左半单环，并设$R=B_1\oplus\cdots\oplus B_m$是由$R$的某个极小左理想的直和分解形成的单分量分解．假设$R=B_1'\times\cdots\times B_t'$，其中每个$B_\ell'$是双边理想而且也是单环．根据引理8.61，每个双边理想B_ℓ'是若干B_i的直和．但B_ℓ'的直和项B_i不能多于一个，否则单环B_ℓ'包含真非零双边理想．所以，$t=m$，且重新标号后对一切i有$B_i'=B_i$.

抛弃下标，剩下的是证明如果$B=\mathrm{Mat}_n(\Delta)\cong\mathrm{Mat}_{n'}(\Delta')=B'$，则$n=n'$且$\Delta\cong\Delta'$．在命题8.49中，我们证明了$\mathrm{Col}(\ell)$（由除第$\ell$列外其他列都是0的一切矩阵组成）是$B$中的极小左理想，从而$\mathrm{Col}(\ell)$是单$B$-模．所以，

$$\{0\}\subseteq\mathrm{Col}(1)\subseteq\mathrm{Col}(1)\oplus\mathrm{Col}(2)\subseteq\cdots\subseteq\mathrm{Col}(1)\oplus\cdots\oplus\mathrm{Col}(n)=B$$

是B作为它自身上的模的一个合成列．根据若尔当-赫尔德定理（定理8.18），n和因子模$\mathrm{Col}(\ell)$是B的不变量．现在根据系8.63，对一切ℓ，$\mathrm{Col}(\ell)\cong\mathrm{Col}(1)$，因此只需证明$\Delta$可以从$\mathrm{Col}(1)$重新得到，而在系8.63（ⅰ）中已经做到了：$\Delta\cong\mathrm{End}_B(\mathrm{Col}(1))^{\mathrm{op}}$. ■

当域k是代数闭域时，对群代数KG的描述可以简化．

567

系8.65（Molien）　*如果G是有限群，k是代数闭域，它的特征不能整除$|G|$，则*

$$kG\cong\mathrm{Mat}_{n_1}(k)\times\cdots\times\mathrm{Mat}_{n_m}(k).$$

证明　根据Maschke定理，kG是半单环，它的单分量同构于形如$\mathrm{Mat}_n(\Delta)$的矩阵环，其中Δ

是 kG 中某个极小左理想 L 的 $\mathrm{End}_{kG}(L)^{\mathrm{op}}$. 所以只要证明 $\mathrm{End}_{kG}(L)^{\mathrm{op}}=\Delta=k$.

现在 $\mathrm{End}_{kG}(L)^{\mathrm{op}} \subseteq \mathrm{End}_k(L)^{\mathrm{op}}$，因 L 是 k 上的有限维向量空间，所以 $\mathrm{End}_k(L)^{\mathrm{op}}$ 也是 k 上的有限维向量空间，因此 $\Delta=\mathrm{End}_{kG}(L)^{\mathrm{op}}$ 是 k 上的有限维向量空间．每个 $f \in \mathrm{End}_{kG}(L)$ 是一个 kG-映射，因此是一个 k-映射；即对一切 $a \in k$ 和 $u \in L$，$f(au)=af(u)$．所以由 $u \mapsto au$ 给出的映射 $\varphi_a: L \to L$ 与 f 可交换；即 k(等同于一切 φ_a) 包含在 Δ 的中心 $Z(\Delta)$ 中．如果 $\delta \in \Delta$，则 δ 和 k 中的每个元素可交换，因此由 k 和 δ 生成的子除环 $k(\delta)$ 是一个（交换）域．由于 Δ 是 k 上的有限维向量空间，从而 $k(\delta)$ 也是 k 上的有限维向量空间；即 $k(\delta)$ 是域 k 的有限扩张，因此根据命题 3.117，δ 是 k 上的代数元素．但 k 是代数闭的，因此 $\delta \in k$ 且 $\Delta=k$. ■

例 8.66 存在不同构的有限群 G 和 H，它们有同构的复数群代数．如果 G 是 n 阶阿贝尔群，则因 $\mathbb{C}$ 是代数闭的，所以 $\mathbb{C}G$ 是 $\mathbb{C}$ 上的矩阵环的直积．而 G 是阿贝尔群蕴涵 $\mathbb{C}G$ 是交换的，因此 $\mathbb{C}G$ 是 $\mathbb{C}$ 的 n 个复制的直积．由此，如果 H 是任一 n 阶阿贝尔群，则 $\mathbb{C}G \cong \mathbb{C}H$. 特别地，$\mathbb{I}_4$ 和 $\mathbb{I}_2 \oplus \mathbb{I}_2$ 是不同构的群，它们有同构的复数群代数．由该例可知，群 G 的某种性质会在群代数 $\mathbb{C}G$ 中消失． ■

系 8.67 *如果 G 是有限群，k 是代数闭域，它的特征不能整除 $|G|$，则 $|G|=n_1^2+n_2^2+\cdots+n_m^2$，其中 kG 的第 i 个单分量 B_i 由 $n_i \times n_i$ 矩阵组成．此外，我们可以假定 $n_1=1$*[⊖].

注 *定理 8.149 说一切 n_i 都是 $|G|$ 的因数．*

证明 作为 k 上的向量空间，kG 和 $\mathrm{Mat}_{n_1}(k)\times\cdots\times\mathrm{Mat}_{n_m}(k)$ 有相同的维数，这是因为根据系 8.65，它们是同构的．但 $\dim(kG)=|G|$，右端的维数是 $\sum_i \dim(\mathrm{Mat}_{n_i}(k))=\sum_i n_i^2$.

最后，例 8.55 证明存在唯一极小左理想同构于平凡模 $V_0(k)$，对应的单分量，比如 B_1 是一维的，因此 $n_1=1$. ■

$\mathbb{C}G$ 中单分量的个数 m 有群论的解释，我们先来求群代数的中心．

定义 *设 $C_1,\cdots,C_r$ 是有限群 G 中的共轭类．对每个 C_j，定义***类和***为元素 $z_j \in \mathbb{C}G$，它由*

$$z_j=\sum_{g \in C_j} g$$

568 *给出．*

下面是共轭类个数 c 的环论解释．

引理 8.68 *如果 r 是有限群 G 中共轭类的个数，则*

$$r=\dim_{\mathbb{C}}(Z(\mathbb{C}G)),$$

其中 $Z(\mathbb{C}G)$ 是群代数的中心．事实上，$Z(\mathbb{C}G)$ 的基由一切类和组成．

证明 如果 $z_j=\sum_{g \in C_j} g$ 是一个类和，则我们断言 $z_j \in Z(\mathbb{C}G)$．如果 $h \in G$，则 $hz_jh^{-1}=z_j$，这是因为用 G 的任一元素作共轭只是共轭类中元素的置换．注意，如果 $j \neq \ell$，则 z_j 和 z_ℓ 没有共同的非零分量，因此 z_1，…，z_r 是一个线性无关表．剩下的要证明 z_j 张成中心．

设 $u=\sum_{g \in G} a_g g \in Z(\mathbb{C}G)$．如果 $h \in G$，则 $huh^{-1}=u$，因此对一切 $g \in G$ 有 $a_{hgh^{-1}}=a_g$. 于是，如果 g 和 g' 在 G 的同一个共轭类中，则它们在 u 中的系数相同，这就说明 u 是类和 z_j 的线性组合． ■

定理 8.69 *如果 G 是有限群，则 $\mathbb{C}G$ 中单分量的个数 m 等于 G 中共轭类的个数 r.*

⊖ 根据例 8.55，群代数 kG 恒有唯一的极小左理想同构于 $V_0(k)$，即使 k 不是代数闭的．

证明　我们在引理 8.68 中刚看到 $r=\dim_{\mathbb{C}}(Z(\mathbb{C}G))$．另一方面，矩阵环的中心 $Z(\mathrm{Mat}_{n_i}(\mathbb{C}))$ 是一切标量矩阵的子空间，因此根据习题 8.12（ⅲ），$m=\dim_{\mathbb{C}}(Z(\mathbb{C}G))$． ■

本节的开始我们看到群 G 的 k-表示对应 kG-模．现在我们回到表示．

定义　*称群 G 的 k-表示是不可约的，如果对应的 kG-模是单的．*

例如，一个一维（必不可约）k-表示是群同态 $\lambda: G\to k^{\times}$，其中 $k^{\times}$ 是 k 的非零元素的乘法群．平凡 kG-模 $V_0(k)$ 对应表示：对一切 $g\in G$，$\lambda_g=1$．

下一结果是构造有限群的特征表的基础．

定理 8.70　*如果 G 是有限群，则它的不可约复数表示的个数等于它的共轭类的个数 r.*

证明　根据命题 8.54，每个单$\mathbb{C}G$-模同构于一个极小左理想．因极小左理想的个数是 m [$\mathbb{C}G$的单分量的个数]，我们知道 m 是 G 的不可约$\mathbb{C}$-表示的个数．而定理 8.69 说 m 等于 G 中共轭类的个数 r． ■ 569

例 8.71　（ⅰ）如果 $G=S_3$，则$\mathbb{C}G$是六维的．因为 S_3 有三个共轭类（根据定理 2.9，S_n 中共轭类的个数等于不同循环结构的个数），所以有三个单分量，维数分别为1,1和 4.（不用定理 8.69 也能知道这个事实，因为把 6 写作平方和，除了六个 1 的和之外，只有一种方式）. 所以

$$\mathbb{C}S_3\cong\mathbb{C}\times\mathbb{C}\times\mathrm{Mat}_2(\mathbb{C}).$$

一维不可约表示中的一个是平凡表示，另一个是 sgn（符号函数）.

（ⅱ）我们现在对 $G=\mathbf{Q}$（8 阶的四元数群）分析 kG. 如果 $k=\mathbb{C}$，则系 8.65 给出

$$\mathbb{C}\mathbf{Q}\cong\mathrm{Mat}_{n_1}(\mathbb{C})\times\cdots\times\mathrm{Mat}_{n_r}(\mathbb{C}),$$

而系 8.67 给出

$$|\mathbf{Q}|=8=n_1^2+n_2^2+\cdots+n_r^2,$$

其中 $n_1=1$. 由此，或者一切 $n_i=1$，或者四个 $n_i=1$ 和一个 $n_i=2$. 第一种情形不可能发生，因为这将蕴涵$\mathbb{C}\mathbf{Q}$ 是交换环，但四元数群 $\mathbf{Q}$ 不是阿贝尔群．所以

$$\mathbb{C}\mathbf{Q}\cong\mathbb{C}\times\mathbb{C}\times\mathbb{C}\times\mathbb{C}\times\mathrm{Mat}_2(\mathbb{C}).$$

我们也可以用定理 8.59，因为 $\mathbf{Q}$ 恰有五个共轭类，就是 $\{1\},\{\bar{1}\},\{i,\bar{i}\},\{j,\bar{j}\},\{k,\bar{k}\}$.

群代数$\mathbb{R}\mathbf{Q}$ 比较复杂，因为$\mathbb{R}$ 不是代数闭的．习题 8.20 证明$\mathbb{H}$ 是$\mathbb{R}\mathbf{Q}$ 的商，由于$\mathbb{R}\mathbf{Q}$ 是半单的，因此$\mathbb{H}$ 同构于$\mathbb{R}\mathbf{Q}$ 的一个直和项．由此，

$$\mathbb{R}\mathbf{Q}\cong\mathbb{R}\times\mathbb{R}\times\mathbb{R}\times\mathbb{R}\times\mathbb{H}.$$ ■

下面是韦德伯恩-阿廷定理的一个爽心的应用．

命题 8.72　*设 R 是环，它的单位元素群 $U=U(R)$ 是有限的且阶为奇数，则 U 是阿贝尔群，且存在正整数 m_i 使得*

$$|U|=\prod_{i=1}^{t}(2^{m_i}-1).$$

证明　首先我们注意到在 R 中 $1=-1$，否则 -1 是偶数阶的单位．考虑群代数 kU，其中 $k=\mathbb{F}_2$．因 k 有特征 2 且 $|U|$ 是奇数，Maschke 定理说 kU 是半单的．存在环映射 $\varphi: kU\to R$ 把 U 中元素的每个 k-线性组合带到“它自身”．现在 $R'=\mathrm{im}\varphi$ 是包含 U 的 R 的子环（因为 kU 有限），因为局限于子环不会制造任何新的单位，所以 $U=U(R')$. 根据系 8.43（ⅲ），环 R'是半单的，因此韦德伯恩-阿廷定理 I 给出 570

$$R'\cong\prod_{i=1}^{t}\mathrm{Mat}_{n_i}(\Delta_i),$$

其中每个 Δ_i 都是除环.

现在因 R'是有限的，所以 Δ_i 是有限的，从而 Δ_i 是有限除环. 根据"另一个"韦德伯恩定理，即定理 8.23，每个 Δ_i 都是域. 但在 R 中 $-1=1$ 蕴涵在 Δ_i 中 $-1=1$，因此每个域 Δ_i 有特征 2；由此对整数 $m_i \geqslant 1$ 有

$$|\Delta_i| = 2^{m_i}.$$

所有的矩阵环必定都是 1×1 的，这是因为较大的矩阵环必包含一个 2 阶元素，就是 $I+K$，其中 K 是最后一行第一个元素为 1 而其他元素为 0 的矩阵. 例如，

$$\begin{bmatrix}1 & 0\\1 & 1\end{bmatrix}^2 = \begin{bmatrix}1 & 0\\2 & 1\end{bmatrix} = I.$$

所以 R'是特征 2 的有限域的直积，从而 $U=U(R')$ 是一个阿贝尔群，它的阶如命题中所述. ■

由此，比如说，恰有五个单位的环是不存在的.

*雅各布森-谢瓦莱稠密性定理*在 20 世纪 30 年代得到证明，它是韦德伯恩定理对某种非阿廷环的重要推广. 环 R 称为**左本原环**，如果存在忠实单左 R-模 S；即 S 是单模，并且如果 $r\in R$ 和 $rS=\{0\}$，则 $r=0$. 可以证明交换本原环是域，而左阿廷左本原环是单的. 现在假定 R 是左本原环，S 是忠实单左 R-模，用 Δ 表示除环 $\mathrm{End}_R(S)$. 稠密性定理表明，如果 R 是左阿廷的，则 $R\cong \mathrm{Mat}_n(\Delta)$，而如果 R 不是左阿廷的，则对每个整数 $n>0$，存在 R 的子环 R_n 使得 $R_n\cong\mathrm{Mat}_n(\Delta)$. 读者可参考 Lam 所著的《A First Course in Noncommutative Rings》，191～193 页.

韦德伯恩-阿廷定理引导了几个领域的研究，其中两个是描述除环和描述有限维代数的. 除环将在第 9 章的中心单代数和第 10 章的叉积代数中考虑，现在我们讨论有限维代数.

由于 Maschke 和 Molien 的定理，韦德伯恩-阿廷定理可以应用到有限群 G 的常表示；即应用到 kG-模上，其中 k 是特征不能整除 $|G|$ 的域. 我们知道此时 kG 是半单的. 然而，模表示，即 k 的特征整除 $|G|$ 的 kG-模自然地产生了. 例如，如果 G 是有限 p-群，其中 p 是某个素数，则极小正规子群 N 是$\mathbb{F}_p$ 上的向量空间. 现在 G（通过共轭）作用在 N 上，因此 N 是$\mathbb{F}_pG$-模. 在有限单群

571

的分类中广泛地使用模表示. 布饶尔（R. Brauer）在模表示的研究中看到不可分解模 M 比不可约模更重要. 回忆模 M 是不可分解的，如果没有非零模 A 和 B 使得 $M=A\oplus B$（在通常情形下，一个模是不可分解的当且仅当它是不可约的［即单的］，但在模的情形下不再成立）. 当 kG 是半单的时候，命题 8.54 说只有有限个不可分解模（对应于极小左理想）. 然而，这在模的情形下不真. 例如，如果 k 是特征 2 的一个代数闭域，$k\mathbf{V}$ 和 kA_4 有无限个不同构的不可分解模.

称域 k 上的一个有限维 k 代数 R **有有限表示型**，如果只有有限多个不同构的有限维不可分解R-模. 希格曼（D. G. Higman）证明：如果 G 是有限群，则对每个域 k，kG 有有限表示型当且仅当它的一切西罗子群 G 都是循环群. 20 世纪 50 年代提出了称为 **Brauer-Thrall 猜想**的两个问题. 设 R 是非有限表示型的环.

（Ⅰ）不可分解 R-模的维数是无界的吗？

（Ⅱ）是否存在严格递增序列 $n_1, n_2, \cdots$，对每个 i 有无限多个不同构的维数为 n_i 的不可分解的 R-模？

1968 年，A. V. Roiter 对第一个猜想给出了有重大影响的肯定回答. 紧随其后，P. Gabriel 引入了图论方法，把有限维代数和某种称为箭图的有向图联系起来. 他证明了一个连通箭图具有有限多个不同构的有限维表示当且仅当该箭图是邓肯（Dynkin）图 A_n, D_n, E_6, E_7 或 E_8 之一（邓肯图是描述复单李代数的多重图，见 778 页的讨论）. Gabriel 的结果可以用遗传 k-代数 A（单边理想是投射

A-模）重新表示．V. Dlab 和 C. Ringel 把 Gabriel 的结果推广到一切邓肯图（通过 G 的任意型 A）．他们证明了一个有限维遗传代数具有有限表示型当且仅当它的图是邓肯图的有限并．此外，用考克斯特函子（它是由 I. N. Bernstein，I. M. Gelfand 和 V. A. Ponomarev 为了给出 Gabriel 结果一个新的证明而引入），他们用所谓的广义邓肯图把分类推广到温顺表示型的遗传代数（无限表示型代数分为温顺型和野型两类）．随后，第二个 Brauer-Thrall 猜想的确认是对一切遗传代数推出的．对代数闭域上的一切（不必是遗传的）有限维代数的 Brauer-Thrall II 的肯定解答来自 R. Bautista，P. Gabriel，A. V. Roiter 和 L. Salmerón 的可乘基定理：每个有限表示型的有限维 k-代数有可乘基 B：A的一个向量空间的基满足两个基向量的积在 $B\cup\{0\}$ 中．事实上，他们证明了存在可乘基，它包含本原正交幂等元的完全集以及根基的每个幂的一个基．M. Auslander 和 I. Reiten 创立了涉及殆分裂序列（定义在第 10 章中）和奥斯兰德-赖滕箭图的理论，这个理论推广了考克斯特函子的概念，提供了（任意）有限维代数的新的不可分解表示的构造．从此，奥斯兰德-赖滕（Auslander-Reiten）理论成为研究有限维代数表示的最有力的工具．对于这些思想的讨论，读者可参考 Artin-Nesbitt-Thrall 所著的《Rings with Minimum Condition》，Dlab-Ringel 所著的《Indecomposable Representations of Graphs and Algebras》，Memoir AMS #173，1976，Jacobson 所著的《The Theory of Rings》，Jacobson 所著的《Structure of Ring》，Drozd-Kirichenko 所著的《Finite Dimensional Algebras》．

572

习题

8.36　设 A 是域 k 上的 n 维 k-代数．证明 A 可以作为 $\mathrm{Mat}_n(k)$ 的 k-子代数嵌入 $\mathrm{Mat}_n(k)$．

提示：如果 $a\in A$，定义 $L_a: A\to A$ 为 $L_a: x\mapsto ax$．

8.37　设 G 是有限群，并设 k 是交换环．定义 $\varepsilon: kG\to k$ 为

$$\varepsilon(\sum_{g\in G} a_g g)=\sum_{g\in G} a_g$$

（这个映射叫做**增广映射**，它的核叫做**增广理想**，记为$\mathcal{G}$）．

（i）证明 ε 是 kG-映射，且作为 k-代数有 $kG/\mathcal{G}\cong k$．由此推出$\mathcal{G}$是 kG 中的双边理想．

（ii）证明 $kG/\mathcal{G}\cong V_0(k)$，其中 $V_0(k)$ 是看作平凡 kG-模的 k．

提示：$\mathcal{G}$是包含 $xu-u=(x-1)u\in\mathcal{G}$的双边理想．

（iii）用（ii）证明：如果 $kG=\mathcal{G}\oplus V$，则 $V=\langle v\rangle$，其中 $v=a\sum_{g\in G} g$．

提示：如同例 8.55 那样论证．

（iv）假定 k 是特征 p 整除 $|G|$ 的域．证明 kG 不是左半单的．

提示：首先证明 $\varepsilon(v)=0$，然后证明短正合列

$$0\to\mathcal{G}\to kG\xrightarrow{\varepsilon} k\to 0$$

不分裂．

8.38　如果 Δ 是除环，证明 $\mathrm{Mat}_n(\Delta)$ 中的每两个极小左理想同构．（与系 8.50 作比较．）

8.39　环 R 中的一个元素 a 叫做**零因子**，如果 $a\neq 0$ 且存在非零 $b\in R$ 使得 $ab=0$（精确地说，a 叫做左零因子，b 叫做右零因子）．证明一个没有零因子的左阿廷环 R 必是除环．

8.40　设 $T: V\to V$ 是线性变换，其中 V 是域 k 上的向量空间，又定义 $k[T]$ 为

$$k[T]=k[x]/(m(x)),$$

其中 $m(x)$ 是 T 的极小多项式．

（i）如果 $m(x)=\prod_p p(x)^{e_p}$，其中 $p(x)\in k[x]$是不同的不可约多项式，且 $e_p\geqslant 1$，证明$k[T]\cong$

573

$\prod_p k[x]/(p(x)^{e_p})$.

（ⅱ）证明 $k[T]$ 是半单环当且仅当 $m(x)$ 是不同线性因式的积．（在线性代数中，我们证明上面的条件等价于 T 是可对角化的，即 T 的任一矩阵［从 T 的某个选定的基产生的］相似于对角矩阵．）

8.41 如果 $G=D_8$，即 8 阶二面体群，求$\mathbb{C}G$.

8.42 如果 $G=A_4$，求$\mathbb{C}G$.

提示： A_4 中有四个共轭类．

8.43 （ⅰ）设 k 是域，并认为 $\mathrm{sgn}: S_n \to \{\pm 1\} \leqslant k$. 定义 $\mathrm{Sig}(k)$为做成 kS_n -模的 k（如同命题 8.37）：如果 $\gamma \in S_n$ 和 $a \in k$，则 $\gamma a = \mathrm{sgn}(\gamma) a$. 证明 $\mathrm{Sig}(k)$是一个不可约 kS_n -模．又，如果 k 的特征不是 2，则 $\mathrm{Sig}(k) \not\cong V_0(k)$.

（ⅱ）求$\mathbb{C}S_5$.

提示： S_5 中有 5 个共轭类．

8.44 设 G 是有限群，并设 k 和 K 都是代数闭域，它们的特征 p 和 q 都不能整除 $|G|$.

（ⅰ）证明 kG 和 KG 的单分量的个数相等．

（ⅱ）证明 G 在 k 上的不可约表示的次数和 G 在 K 上的不可约表示的次数相等．

8.4 张量积

我们现在介绍一个新的概念，㊀即张量积，它用来构造诱导表示（它把子群的表示扩张为整个群的表示）．张量积在代数的其他领域也十分有用，例如它们涉及双线性型、伴随同构、自由代数、外代数和行列式．希望立即知道韦德伯恩-阿廷定理和 Maschke 定理对于群的影响的读者可以直接跳到下一节，因为我们将给出的第一个应用——伯恩赛德定理——在证明中没有用到诱导表示．另一方面，我们也将证明弗罗贝尼乌斯的定理，那是要用到诱导表示的．

如果 k 是域，H 是群 G 的子群，则 H 的一个 k -表示和一个 kH -模是同一个东西，G 的一个 k -表示和一个 kG -模是同一个东西．如果能够迫使一个 kH -模 M 成为一个 kG -模，则可以从子群的表示造出大群 G 的表示．更一般地，如果 A 是环 R 的子环，我们要迫使一个 A -模 M 成为一个 R-模．如果 M 是由集合 X 生成的 A -模，则每个 $m \in M$ 有形如 $m=\sum_i a_i x_i$ 的表达式，其中 $a_i \in A$，

574

$x_i \in X$. 或许我们可以取形如 $\sum_i r_i x_i$ 的一切表达式，其中 $r_i \in R$，以此来造出一个包含 M 的 R-模．这个天真的方法注定要失败．例如，一个 n 阶循环群 $G=\langle g \rangle$ 是一个$\mathbb{Z}$-模，我们能够使它成为一个$\mathbb{Q}$-模吗？一个$\mathbb{Q}$-模 V 是$\mathbb{Q}$上的向量空间，易知如果 $v \in V$ 和 $q \in \mathbb{Q}$，则 $qv=0$ 当且仅当 $q=0$ 或 $v=0$. 如果能够用上面描述的天真方法造出一个包含 G 的有理向量空间 V，则 $ng=0$ 会导出在 V 中 $g=0$！添加标量来获得大环上的模的目标仍然有价值，不过很明显我们不能对它的构造如此大度．对此可行的方法是用*张量积*．

引入张量积最注目的理由之一来自代数拓扑，那里对每个拓扑空间 X 指定了一个*同调群*的序列 $H_n(X)$，其中所有 $n \geqslant 0$，它是代数拓扑的重要基础．*屈内特*(Künneth) *公式*计算了两个拓扑空间的笛卡儿积 $X \times Y$ 的同调群，该公式就是用了因子 X 和 Y 的同调群的张量积．

㊀ R-模的张量积，其中 R 是交换环，可以在第 7 章中引入．然而，将其延迟到本章介绍了非交换环之后，相信会得到更好的展示．如果把张量积放到较早的地方介绍，就必须分两步构造它们：先在第 7 章的交换环上构造，然后现在再在一般环上构造．这不是一个好的想法．

定义　设 R 是环，A_R 是右 R-模，${}_RB$ 是左 R-模，并设 G 是（加法）阿贝尔群．函数 $f: A\times B\to G$ 叫做 R-**双加性的**，如果对一切 $a,a'\in A, b,b'\in B$ 和 $r\in R$，有

$$f(a+a',b)=f(a,b)+f(a',b);$$
$$f(a,b+b')=f(a,b)+f(a,b');$$
$$f(ar,b)=f(a,rb).$$

R-双加性函数也叫做**配对函数**.

如果 R 是交换环，A,B 和 M 是 R-模，则函数 $f: A\times B\to M$ 叫做 R-**双线性的**，如果它是 R-双加性的且

$$f(ar,b)=f(a,rb)=rf(a,b).$$

例 8.73　（ⅰ）如果 R 是环，则它的乘法 $\mu: R\times R\to R$ 是 R-双加性的，第一和第二两个公理是左右分配律，而第三个公理是结合性：

$$\mu(ar,b)=(ar)b=a(rb)=\mu(a,rb).$$

如果 R 是交换环，则 μ 是 R-双线性的，因为 $(ar)b=a(rb)=r(ab)$.

（ⅱ）如果 ${}_RM$ 是左 R-模，则它的标量乘法 $\sigma: R\times M\to M$ 是 R-双加性的；如果 R 是交换环，则 σ 是 R-双线性的．

（ⅲ）如果 M_R 和 N_R 都是右 R-模，对 $f\in \mathrm{Hom}_R(M,N)$ 和 $r\in R$ 定义 $rf: M\to N$ 为

$$rf: m\mapsto f(mr),$$

则 $\mathrm{Hom}_R(M,N)$ 是左 R-模．读者可以证明这样确实使 Hom 成为左 R-模．此外，我们现在可以看到由 $(m,f)\mapsto f(m)$ 给出的赋值函数 $e: M\times \mathrm{Hom}_R(M,N)\to N$ 是 R-双加性的． 575

域 k 上的向量空间 V 的对偶空间 V^* 给出这个构造的一个特殊情形：赋值函数 $V\times V^*\to k$ 是 R-双线性的．

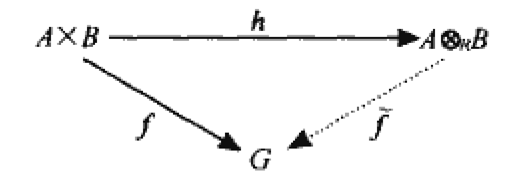
（ⅳ）如果 $G^*=\mathrm{Hom}_{\mathbb{Z}}(G,\mathbb{Q}/\mathbb{Z})$ 是阿贝尔群 G 的庞特里亚金（Pontrjagin）对偶，则赋值函数 $G\times G^*\to\mathbb{Q}/\mathbb{Z}$ 是 $\mathbb{Z}$-双线性的． ■

张量积把双加性函数转变为双线性函数．

定义　给定环 R 和模 A_R，${}_RB$，则它们的**张量积**是指一个阿贝尔群 $A\otimes_R B$ 和一个 R-双加性函数

$$h: A\times B\to A\otimes_R B$$

满足对每个阿贝尔群 G 和每个 R-双加性函数 $f: A\times B\to G$，存在唯一的 $\mathbb{Z}$-同态 $\tilde{f}: A\otimes_R B\to G$ 使得下图交换：



如果 A 和 B 的张量积存在，则不计同构是唯一的，因为它已经定义为一个泛映射问题的解（见命题 7.27 的证明）.

当 $R=\mathbb{Z}$ 时，我们常把 $A\otimes_R B$ 记为 $A\otimes B$.

命题 8.74　如果 R 是环，A_R 和 ${}_RB$ 都是模，则它们的张量积存在．

证明　设 F 是以 $A\times B$ 为基的自由阿贝尔群；即 F 在一切有序对 (a,b) 上是自由的，其中 $a\in A$ 和 $b\in B$．定义 S 为由下列类型

$$(a,b+b')-(a,b)-(a,b');$$
$$(a+a',b)-(a,b)-(a',b);$$
$$(ar,b)-(a,rb)$$

的一切元素生成的 F 的子群．定义 $A\otimes_R B=F/S$，记陪集$(a,b)+S$ 为 $a\otimes b$，且定义

$$h: A\times B\to A\otimes_R B \text{ 为 } h:(a,b)\mapsto a\otimes b$$

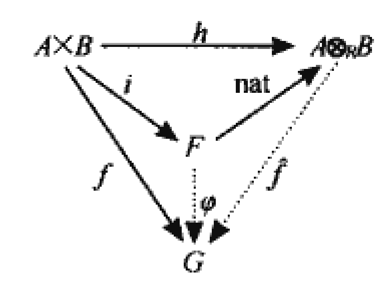
（这样，h 是自然映射 $F\to F/S$ 的限制）．在 $A\otimes_R B$ 中我们有下列恒等式：

$$a\otimes(b+b')=a\otimes b+a\otimes b';$$
$$(a+a')\otimes b=a\otimes b+a'\otimes b;$$
$$ar\otimes b=a\otimes rb.$$

576

现在显然 h 是 R-双加性的．

考虑下面的图，其中 G 是阿贝尔群，f 是 R-双加性的：



其中 $i: A\times B\to F$ 是包含映射，nat 是自然映射．因 F 是以 $A\times B$ 为基的自由阿贝尔群，存在同态 $\varphi: F\to G$ 使得对一切 (a,b)，$\varphi(a,b)=f(a,b)$．现在因 f 是 R-双加性的，所以 $S\subseteq\ker\varphi$，从而 φ 由

$$\hat{f}(a\otimes b)=\hat{f}((a,b)+S)=\varphi(a,b)=f(a,b)$$

诱导出一个映射 $\hat{f}: A\otimes_R B\to G$（因为 $A\otimes_R B=F/S$）．上面的等式可以写作 $\hat{f}h=f$；即图交换．最后，因为 $A\otimes_R B$ 由一切 $a\otimes b$ 的集合生成，所以 $\hat{f}$ 是唯一的． ■

注 因 $A\otimes_R B$ 由形如 $a\otimes b$ 的元素生成，每个 $u\in A\otimes_R B$ 形如

$$u=\sum_i a_i\otimes b_i.$$

u 的这个表达式是不唯一的，例如有表达式

$$\begin{aligned}0&=a\otimes(b+b')-a\otimes b-a\otimes b'\\&=(a+a')\otimes b-a\otimes b-a'\otimes b\\&=ar\otimes b-a\otimes rb.\end{aligned}$$

所以给定某个阿贝尔群 G，一个映射 $g: A\otimes_R B\to G$ 由指定 g 在生成元 $a\otimes b$ 上的值来定义必定是有疑问的，这样一个"函数" g 或许不是合理定义的，因为用生成元来表达元素有许多表达式．本质上，g 只是定义在 F 上的（以 $A\times B$ 为基的自由阿贝尔群），因为 $A\otimes_R B=F/S$，我们还必须证明 $g(S)=\{0\}$．最简单的（也是最安全的）方法是在 $A\times B$ 上定义一个 R-双加性函数，它将产生一个（合理定义的）同态．在下一个证明中，我们解释这个方法．

命题 8.75 设 $f: A_R\to A'_R$ 和 $g: {}_RB\to {}_RB'$ 分别是右 R-模和左 R-模的映射，则存在唯一的 $\mathbb{Z}$-同态，记为 $f\otimes g: A\otimes_R B\to A'\otimes_R B'$，使得

577

$$f\otimes g: a\otimes b\mapsto f(a)\otimes g(b).$$

证明 易知由$(a,b)\mapsto f(a)\otimes g(b)$给出的函数 $\varphi: A\times B\to A'\otimes_R B'$ 是一个 R-双加性函数.

例如，

$$\varphi:(ar,b)\mapsto f(ar)\otimes g(b)=f(a)r\otimes g(b)$$

和

$$\varphi:(a,rb)\mapsto f(a)\otimes g(rb)=f(a)\otimes rg(b);$$

因为在 $A'\otimes_R B'$中有恒等式 $a'r\otimes b'=a'\otimes rb'$，所以两者相等．双加性函数 φ 产生唯一的同态 $A\otimes_R B\to A'\otimes_R B'$ 使得

$$a\otimes b\mapsto f(a)\otimes g(b).$$ ■

系 8.76　给定右 R-模的映射 $A\xrightarrow{f}A'\xrightarrow{f'}A''$和左 R-模的映射 $B\xrightarrow{g}B'\xrightarrow{g'}B''$，

$$(f'\otimes g')(f\otimes g)=f'f\otimes g'g.$$

证明　两个映射都把 $a\otimes b\mapsto f'f(a)\otimes g'g(b)$，这种同态的唯一性给出所要的等式． ■

定理 8.77　给定 A_R，存在加性函子 $F_A:{}_R\mathbf{Mod}\to\mathbf{Ab}$，定义为

$$F_A(B)=A\otimes_R B\text{ 和 }F_A(g)=1_A\otimes g,$$

其中 $g:B\to B'$ 是左 R-模的映射．

证明　首先，注意 F_A 保持幺元：$F_A(1_B)=1_A\otimes 1_B$，因为它固定每个生成元 $a\otimes b$，所以它是幺元 $1_{A\otimes B}$．其次，F_A 保持复合：根据系 8.76，有

$$F_A(g'g)=1_A\otimes g'g=(1_A\otimes g')(1_A\otimes g)=F_A(g')F_A(g),$$

所以 F_A 是函子．

为证明 F_A 是加性的，需要证明 $F_A(g+h)=F_A(g)+F_A(h)$，其中 $g,h:B\to B'$，即要证明 $1_A\otimes(g+h)=1_A\otimes g+1_A\otimes h$．因为两个映射都把 $a\otimes b\mapsto a\otimes g(b)+a\otimes h(b)$，所以等式成立． ■

我们记函子 F_A 为 $A\otimes_R$．当然，如果固定一个左 R-模，就有一个类似的结果：存在加性函子 $\otimes_R B:\mathbf{Mod}_R\to\mathbf{Ab}$.

系 8.78　如果 $f:M\to M'$ 和 $g:N\to N'$ 分别是右 R-模和左 R-模的同构，则 $f\otimes g:M\otimes_R N\to M'\otimes_R N'$ 是阿贝尔群的同构．

[578]

证明　现在 $f\otimes 1_{N'}$是函子 $F_{N'}$ 在同构 f 上的值，因此 $f\otimes 1_{N'}$是同构，同样，$1_M\otimes g$ 是同构．根据系 8.76，有 $f\otimes g=(f\otimes 1_{N'})(1_M\otimes g)$．所以 $f\otimes g$ 是同构的复合，也是同构． ■

在继续陈述张量积的性质之前，我们暂时讨论一个技术问题．一般来说，两个模的张量积只是一个阿贝尔群，它有可能是模吗？如果是模，那么张量积函子是否不仅在 **Ab** 中取值，而且也在模范畴中取值？即 $1\otimes f$ 恒为模映射吗？

定义　设 R 和 S 是环，并设 M 是阿贝尔群．则称 M 是 (R,S)-双模（记为 ${}_RM_S$），如果 M 既是左 R-模又是右 S-模，且两个标量乘法由一个结合律联系起来：对一切 $r\in R,m\in M$ 和 $s\in S$，

$$r(ms)=(rm)s.$$

如果 M 是(R,S)-双模，可以写 rms 而不加括号，因为双模的定义说两个可能的结合是一致的．

例 8.79　（ⅰ）每个环 R 是一个 (R,R)-双模，额外的恒等式就是 R 中乘法的结合性．

（ⅱ）环 R 中的每个双边理想都是 (R,R)-双模．

（ⅲ）如果 M 是左 R-模（即 $M={}_RM$）则 M 是一个$(R,\mathbb{Z})$-双模，即 $M={}_RM_{\mathbb{Z}}$．同样，右 R-模 N 是双模${}_{\mathbb{Z}}N_R$.

（ⅳ）如果 R 是交换环，则每个左（或右）R-模是 (R,R)-双模．详细地说，如果 $M={}_RM$，

定义新的标量乘法 $M\times R\to M$ 为 $(m,r)\mapsto rm$．为证明 M 是右 R-模，我们需要证明 $m(rr')=(mr)r'$，即 $(rr')m=r'(rm)$，因 $rr'=r'r$，该式成立．最后，因为 $r(mr')$ 和 $(rm)r'$ 都等于 $(rr')m$，所以 M 是 (R,R)－双模．

（v）在例 8.6 中，我们把任一左 kG-模 M 做成右 kG-模，方法是对每个 $m\in M$ 和群 G 中的每个 g 定义 $mg=g^{-1}m$．尽管 M 既是左又是右 kG-模，但通常它不是一个 (kG,kG)-双模，因为所要的结合性公式可能不成立．更详细地说，设 $g,h\in G$ 和 $m\in M$．现在 $g(mh)=g(h^{-1}m)=(gh^{-1})m$，另一方面，$(gm)h=h^{-1}(gm)=(h^{-1}g)m$．为明确两者可以不同，取 $M=kG$，$m=1$ 和 g，h 为 G 中不交换的元素． ■

下一引理解决了扩张标量的问题．

引理 8.80 *给定双模 ${}_SA_R$ 和左模 ${}_RB$，则张量积 $A\otimes_R B$ 是一个左 S-模，其中*

[579]

$$s(a\otimes b)=(sa)\otimes b.$$

同样，给定 A_R 和 ${}_RB_S$，张量积 $A\otimes_R B$ 是一个右 S-模，其中 $(a\otimes b)s=a\otimes(bs)$．

特别地，如果 k 是交换环且 A 是 k-代数，则 $A\otimes_k B$ 是一个左 A-模．

证明 对固定的 $s\in S$，由 $a\mapsto sa$ 定义的乘法 $\mu_s: A\to A$ 是一个 R-映射，这是因为 A 是双模给出

$$\mu_s(ar)=s(ar)=(sa)r=\mu_s(a)r.$$

如果 $F=\otimes_R B: \mathbf{Mod}\to\mathbf{Ab}$，则 $F(\mu_s): A\otimes_R B\to A\otimes_R B$ 是（合理定义的）Z-同态．于是 $F(\mu_s)=\mu_s\otimes 1_B: a\otimes b\mapsto(sa)\otimes b$，因此引理陈述中的公式有意义．现在容易直接验证对 $A\otimes_R B$ 模公理成立．

由 k-代数 A 是 (A,k)-双模可得最后一个陈述． ■

例如，如果 V 和 W 都是域 k 上的向量空间，则它们的张量积 $V\otimes_k W$ 也是域 k 上的向量空间．

稍后，我们知道证明张量积的性质就是证明那些明显的映射确是合理定义的函数．

对于最初的问题，我们已经有了一些进展：给定一个左 K-模 M，其中 k 是环 K 的子环，我们可以用扩张标量的方法由 M 造出一个左 K-模；即引理 8.80 表明，因为 K 是一个 (K,k)－双模，所以 $K\otimes_k M$ 是左 K－模．然而，我们还要研究为什么一个左 k-模 M 不能嵌入 $K\otimes_k M$ 中，其中 k 是环 K 的子环．

下面扩张标量的特殊情形对于表示是重要的．如果 H 是群 G 的子群，$\rho: H\to \mathrm{GL}(V)$ 是 k-表示，则 $\rho: H\to\mathrm{GL}(V)$ 把 V 配置成一个左 kH-模结构．我们称 $V^G=kG\otimes_{kH}V$ 为诱导模．注意 kG 是右 kH－模（它甚至还是右 kG-模），所以张量积 $V^G=kG\otimes_{kH}V$ 有意义．此外，由引理 8.80，V^G 是左 kG-模．在本章的后面我们要更仔细地研究这个结构（见 624 页的诱导模）．

系 8.81 （i）*给定双模 ${}_SA_R$，则函子 $F_A=A\otimes_R: {}_R\mathbf{Mod}\to\mathbf{Ab}$ 事实上在 ${}_S\mathbf{Mod}$ 中取值．*

（ii）*如果 R 是交换环，则 $A\otimes_R B$ 是 R-模，其中对一切 $r\in R$，$a\in A$ 和 $b\in B$，*

$$r(a\otimes b)=(ra)\otimes b=a\otimes rb.$$

（iii）*如果 R 是交换环，$r\in R$，$\mu_r: B\to B$ 是乘 r 的映射，则*

$$1_A\otimes\mu_r: A\otimes_R B\to A\otimes_R B$$

[580]

也是乘 r 的映射．

证明 （i）根据引理，我们知道 $A\otimes_R B$ 是左 S-模，其中 $s(a\otimes b)=(sa)\otimes b$，所以只要证明：如果 $g: B\to B'$ 是左 R-模的映射，则 $F_A(g)=1_A\otimes g$ 是 S－映射．而

$$(1_A \otimes g)[s(a \otimes b)] = (1_A \otimes g)[(sa) \otimes b]$$
$$= (sa) \otimes gb$$
$$= s(a \otimes gb) \qquad \text{根据引理 8.80}$$
$$= s(1_A \otimes g)(a \otimes b).$$

（ⅱ）因 R 是交换环，我们可以通过定义 $ar=ra$ 而把 A 看作 (R,R)-双模．现在引理 8.80 给出

$$r(a \otimes b) = (ra) \otimes b = (ar) \otimes b = a \otimes rb.$$

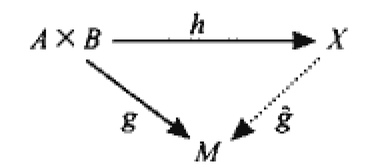
（ⅲ）这个陈述只需从另一个角度来看上面的等式 $a \otimes rb = r(a \otimes b)$：

$$(1_A \otimes \mu_r)(a \otimes b) = a \otimes rb = r(a \otimes b).$$ ■

我们已经对任意的可以是非交换的环 R 定义了 R-双加性函数，而只对交换环定义了 R-双线性函数．张量积定义为涉及 R-双加性函数的某个泛映射问题的解，我们现在考虑当 R 为交换环时对于 R-双线性函数的类似问题．

下面是一个临时定义，很快就会看到没有必要作这个定义．

定义　如果 k 是交换环，则一个 k-**双线性乘积**是指一个 k-模 X 和一个 k-双线性函数 $h: A\times B\to X$，满足对每个 k-模 M 和每个 k-双线性函数 $g: A\times B\to M$，存在唯一的 k-同态 $\hat{g}: X\to M$ 使得下图交换：



下一结果证明 k-双线性乘积存在，但不是新东西．

命题 8.82　如果 k 是交换环，且 A 和 B 是 k-模，则 k-模 $A\otimes_k B$ 是一个 k-双线性乘积．

581

证明　我们证明如果定义 $h((a,b)) = a\otimes b$，则 $X=A\otimes_k B$ 提供解．注意由系 8.81，h 也是 k-双线性的．因 g 是 k-双线性的，所以它是 k-双加性的，从而存在 $\mathbb{Z}$-同态 $\hat{g}: A\otimes_k B\to M$，它对一切 $(a,b)\in A\times B$ 有 $\hat{g}(a\otimes b) = g(a,b)$．我们只需证明 $\hat{g}$ 是 k-映射．如果 $u\in k$，则

$$\hat{g}(u(a\otimes b)) = \hat{g}((ua)\otimes b)$$
$$= g(ua, b)$$
$$= ug(a,b) \qquad \text{因为 } g \text{ 是 } k\text{-双线性的}$$
$$= u\hat{g}(a\otimes b).$$ ■

作为这个命题的一个推论，没有必要给出双线性乘积这个术语，把它叫做张量积就可以了．

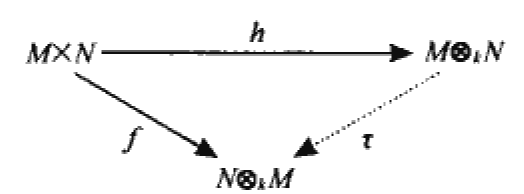
和 Hom 函子对照，张量函子服从某种交换律和结合律．

命题 8.83（交换性）　如果 k 是交换环，M 和 N 是 k-模，则存在 k-同构

$$\tau: M\otimes_k N\to N\otimes_k M,$$

其中 $\tau: m\otimes n\mapsto n\otimes m$.

证明　首先，系 8.81 证明 $M\otimes_k N$ 和 $N\otimes_k M$ 都是 k-模．考虑图



其中 $f(m,n) = n\otimes m$．易知 f 是 k-双线性的，从而存在唯一的 k-映射 $\tau: M\otimes_k N\to N\otimes_k M$ 满足

$\tau: m\otimes n\to n\otimes m$. 交换 $M\otimes_k N$ 和 $N\otimes_k M$ 的角色得到的类似的图给出反方向的 k-映射把 $n\otimes m\to m\otimes n$. 这两个映射的两种复合显然都是恒等映射，所以 τ 是 k-同构. ■

命题 8.84 (结合性)　*给定 A_R, ${}_RB_S$ 和 ${}_SC$，存在同构*

$$\theta: A\otimes_R(B\otimes_S C)\cong(A\otimes_R B)\otimes_S C,$$

它由

$$a\otimes(b\otimes c)\mapsto(a\otimes b)\otimes c$$

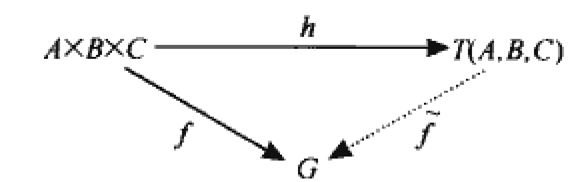
给出.

证明　定义三加性函数 $f: A\times B\times C\to G$，其中 G 是阿贝尔群，为三个变元的每一个（当固定其他两个的时候）都是加性函数，对一切 $r\in R$ 和 $s\in S$,

582

$$f(ar,b,c)=f(a,rb,c) \text{ 和 } f(a,bs,c)=f(a,b,sc).$$

考虑由图



描述的泛映射问题，其中 G 是阿贝尔群，f 是三加性的，$\tilde{f}$ 是$\mathbb{Z}$-同态. 同双加性函数和两个模的张量积一样，定义 $T(A,B,C)=F/N$，其中 F 是一切有序三元组 $(a,b,c)\in A\times B\times C$ 上的自由阿贝尔群，N 是明显的关系子群. 定义 $h: A\times B\times C\to T(A,B,C)$ 为

$$h:(a,b,c)\mapsto(a,b,c)+N$$

(记 $(a,b,c)+N$ 为 $a\otimes b\otimes c$). 容易验证这个构造对三加性函数给出泛映射问题的解.

现在证明 $A\otimes_R(B\otimes_S C)$ 是这个泛问题的另一个解. 定义三加性函数 $\eta: A\times B\times C\to A\otimes_R(B\otimes_S C)$ 为 $\eta:(a,b,c)\mapsto a\otimes(b\otimes c)$，我们需要找出同态 $\tilde{f}: A\otimes_R(B\otimes_S C)\to G$ 使得 $\tilde{f}\eta=f$. 对每个 $a\in A$，定义为 $(b,c)\mapsto f(a,b,c)$ 的 S-双加性函数 $f_a: B\times C\to G$ 给出唯一的同态 $\tilde{f}_a: B\otimes_S C\to G$ 把 $b\otimes c\mapsto f(a,b,c)$. 如果 $a,a'\in A$，则

$$\tilde{f}_{a+a'}(b\otimes c)=f(a+a',b,c)=f(a,b,c)+f(a',b,c)=\tilde{f}_a(b\otimes c)+\tilde{f}_{a'}(b\otimes c).$$

由此定义为 $\varphi(a,b\otimes c)=\tilde{f}_a(b\otimes c)$ 的函数 $\varphi: A\times(B\otimes_S C)\to G$ 对两个变量都是加性的. 它是R-双加性的，这是因为如果 $r\in R$，则

$$\varphi(ar,b\otimes c)=\tilde{f}_{ar}(b\otimes c)=f(ar,b,c)=f(a,rb,c)=\tilde{f}_a(rb\otimes c)=\varphi(a,r(b\otimes c)).$$

所以有唯一的同态 $\tilde{f}: A\otimes_R(B\otimes_S C)\to G$ 满足 $a\otimes(b\otimes c)\mapsto\varphi(a,b\otimes c)=f(a,b,c)$；即 $\tilde{f}\eta=f$. 泛映射问题解的唯一性表明存在满足 $a\otimes b\otimes c\mapsto a\otimes(b\otimes c)$ 的同构 $T(A,B,C)\to A\otimes_R(B\otimes_S C)$. 同样经 $a\otimes b\otimes c\mapsto(a\otimes b)\otimes c$ 有 $T(A,B,C)\cong(A\otimes_R B)\otimes_S C$，因此经 $a\otimes(b\otimes c)\mapsto(a\otimes b)\otimes c$ 有 $A\otimes_R(B\otimes_S C)\cong(A\otimes_R B)\otimes_S C$. ■

注　*元素 $a\otimes b\otimes c\in T(A,B,C)$ 没有括号，将在下一章构造张量代数时给以剖析.*

我们现在给出张量积的性质，这将有助于对它们的计算. 首先，给出关于 Hom 的一个结果，然后给出张量的类似结果.

583

回忆习题 8.34：对任意左 R-模 M，对任意 $f\in \mathrm{Hom}_R(R,M)$ 和任意 $r,s\in R$，定义

$$rf: s\mapsto f(sr).$$

用环 R 是(R,R)-双模的事实可以验证 rf 是R-映射，且 $\mathrm{Hom}_R(R,M)$是左 R-模. 我们把它合并为

下面的结果.

命题 8.85 如果 M 是左 R-模，则 $\mathrm{Hom}_R(R,M)$ 是左 R-模，且由 $\varphi_M(f)=f(1)$ 给出 R-同构 $\varphi_M:\mathrm{Hom}_R(R,M)\to M$. 事实上，$\varphi=\{\varphi_M\}$ 是 $\mathrm{Hom}_R(R,\ )$ 和 ${}_R\mathbf{Mod}$ 上的单位函子之间的自然等价.

证明 修改命题 7.102 的证明即可. ■

命题 8.86 对每个左 R-模 M，存在 R-同构

$$\theta_M: R\otimes_R M\to M,$$

其中 $\theta_M: r\otimes m\mapsto rm$. 事实上，$\theta=\{\theta_M\}$ 是 $R\otimes_R$ 和 ${}_R\mathbf{Mod}$ 上的单位函子之间的自然等价.

证明 由 $(r,m)\mapsto rm$ 给出的函数 $R\times M\to M$ 是 R-双加性的，从而存在 R-同态 $\theta: R\otimes_R M\to M$，其中 $r\otimes m\mapsto rm$ [用 R 是 (R,R)-双模的事实]. 为证明 θ 是 R-同构，只需找出 $\mathbb{Z}$-同态 $f: M\to R\otimes_R M$ 使得 θf 和 $f\theta$ 都是恒等映射（因为现在只有一个问题，就是函数 θ 是否是双射）. 这样的 $\mathbb{Z}$-映射由 $f: m\mapsto 1\otimes m$ 给出.

为证明同构 θ_M 构成自然等价，我们需要证明对任意模同态 $h: M\to N$，下图交换：

$$\begin{array}{ccc} R\otimes_R M & \xrightarrow{1\otimes h} & R\otimes_R N \\ \downarrow{\scriptstyle\theta_M} & & \downarrow{\scriptstyle\theta_N} \\ M & \xrightarrow{h} & N \end{array}$$

为此只要考察 $R\otimes_R M$ 的生成元 $r\otimes m$ 就够了. 顺时针走，$r\otimes m\mapsto r\otimes h(m)\mapsto rh(m)$，而逆时针走，$r\otimes m\mapsto rm\mapsto h(rm)$. 因 h 是 R-映射，有 $h(rm)=rh(m)$，所以两者一致. ■

下一定理说张量积保持任意直和.

定理 8.87 给定右模 A_R 和左 R-模 $\{{}_RB_i: i\in I\}$，存在 $\mathbb{Z}$-同构

$$\varphi: A\otimes_R\sum_{i\in I}B_i\to\sum_{i\in I}(A\otimes_R B_i),$$

其中 $\varphi: a\otimes(b_i)\mapsto(a\otimes b_i)$. 此外，如果 R 是交换环，则 φ 是 R-同构.

证明 因为由 $f:(a,(b_i))\mapsto(a\otimes b_i)$ 给出的函数 $f: A\times\left(\sum_i B_i\right)\to\sum_i(A\otimes_R B_i)$ 是 R-双加性的，所以存在 $\mathbb{Z}$-同态

$$\varphi: A\otimes_R\left(\sum_i B_i\right)\to\sum_i(A\otimes_R B_i)$$

满足 $\varphi: a\otimes(b_i)\mapsto(a\otimes b_i)$. 如果 R 是交换的，则 $A\otimes_R\left(\sum_{i\in I}B_i\right)$ 和 $\sum_{i\in I}(A\otimes_R B_i)$ 都是 R-模且 φ 是 R-映射（因为 φ 是命题 8.82 中的泛映射问题给出的函数）.

为证明 φ 是同构，我们给出它的逆. 记内射 $B_j\to\sum_i B_i$ 为 λ_j [其中 $\lambda_j(b_j)\in\sum_i B_i$ 第 j 个坐标为 b_j，其他坐标为 0]，因此，$1_A\otimes\lambda_j: A\otimes_R B_j\to A\otimes_R\left(\sum_i B_i\right)$. 这个直和是 ${}_R\mathbf{Mod}$ 中的余积，它给出有 $\theta:(a\otimes b_i)\mapsto a\otimes\sum_i\lambda_i(b_i)$ 的同态 $\theta:\sum_i(A\otimes_R B_i)\to A\otimes_R\left(\sum_i B_i\right)$. 现在容易验证 θ 是 φ 的逆，所以 φ 是同构. ■

[584]

有一个 C. E. Watts 的定理（见 Rotman 所著的《An Introduction to Homological Algebra》，77 页）说：如果 $T:{}_R\mathbf{Mod}\to\mathbf{Ab}$ 是一个保持直和的（共变）右正合函子，则存在右 R-模 A 使得 T 和 $A\otimes_R$ 自然等价.

例 8.88 设 k 是域，并设 V 和 W 都是 k-模，即 V 和 W 都是 k 上的向量空间．现在 W 是自由 k-模，比如 $W=\sum_{i\in I}\langle w_i\rangle$，其中 $\{w_i: i\in I\}$ 是 W 的基．所以 $V\otimes_k W\cong\sum_{i\in I}V\otimes_k\langle w_i\rangle$．同样，$V=\sum_{j\in J}\langle v_j\rangle$，其中 $\{v_j: j\in J\}$ 是 V 的基，且对每个 i，$V\otimes_k\langle w_i\rangle\cong\sum_{j\in J}\langle v_j\rangle\otimes_k\langle w_i\rangle$．但一维向量空间 $\langle v_j\rangle$ 和 $\langle w_i\rangle$ 同构于 k，命题 8.86 给出 $\langle v_j\rangle\otimes_k\langle w_i\rangle\cong\langle v_j\otimes w_i\rangle$．因此，$V\otimes_k W$ 是以 $\{v_j\otimes w_i: i\in I, j\in J\}$ 为基的 k 上的向量空间．在 V 和 W 都是有限维的情形，我们有

$$\dim(V\otimes_k W)=\dim(V)\dim(W).$$ ■

例 8.89 我们现在证明在张量积 $V\otimes_k V$ 中可能存在元素不能写作 $u\otimes w$ 的形式，其中 $u,w\in V$．设 v_1,v_2 是域 k 上二维向量空间 V 的基．和例 8.88 一样，$V\otimes_k V$ 的一组基是

$$v_1\otimes v_1, v_1\otimes v_2, v_2\otimes v_1, v_2\otimes v_2.$$

我们断言不存在 $u,w\in V$ 使得 $v_1\otimes v_2+v_2\otimes v_1=u\otimes w$．否则，把 u 和 w 用 v_1 和 v_2 写出来：

$$\begin{aligned}v_1\otimes v_2+v_2\otimes v_1&=u\otimes w\\&=(av_1+bv_2)\otimes(cv_1+dv_2)\\&=acv_1\otimes v_1+adv_1\otimes v_2+bcv_2\otimes v_1+bdv_2\otimes v_2.\end{aligned}$$

由基的线性无关性，

$$ac=0=bd \text{ 和 } ad=1=bc.$$

585

第一个方程给出 $a=0$ 或 $c=0$，不管那种情形，代入第二个方程可得 $0=1$． ■

作为定理 8.87 的一个推论，如果

$$0\to B'\xrightarrow{i}B\xrightarrow{p}B''\to 0$$

是左 R-模的分裂短正合列，则对每个右 R-模 A，

$$0\to A\otimes_R B'\xrightarrow{1_A\otimes i}A\otimes_R B\xrightarrow{1_A\otimes p}A\otimes_R B''\to 0$$

也是分裂短正合列．如果正合列不是分裂的会怎样？

定理 8.90（右正合性） *设 A 是右 R-模，并设*

$$B'\xrightarrow{i}B\xrightarrow{p}B''\to 0$$

是左 R-模的正合列，则

$$A\otimes_R B'\xrightarrow{1_A\otimes i}A\otimes_R B\xrightarrow{1_A\otimes p}A\otimes_R B''\to 0$$

是阿贝尔群的正合列．

注 （i）序列的起始缺少 $0\to$ 将在后面讨论；显然这与初始时把群 G 嵌入 $\mathbb{Q}$ 上向量空间的问题有关．

（ii）一旦证明了伴随同构，就可以给出这个定理的一个更好的证明（见命题 8.100）．

证明 有三点需要验证．

（i）$\operatorname{im}(1\otimes i)\subseteq\ker(1\otimes p)$．

只需证明复合是 0；但

$$(1\otimes p)(1\otimes i)=1\otimes pi=1\otimes 0=0.$$

（ii）$\ker(1\otimes p)\subseteq\operatorname{im}(1\otimes i)$．

设 $E=\operatorname{im}(1\otimes i)$．根据（i），$E\subseteq\ker(1\otimes p)$，从而 $1\otimes p$ 诱导出一个映射 $\hat{p}:(A\otimes B)/E\to A\otimes B''$ 满足

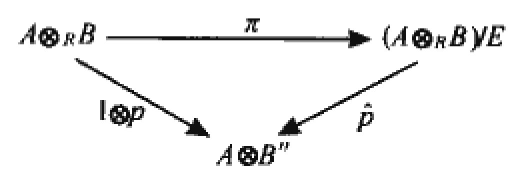
$$\hat{p}: a \otimes b + E \mapsto a \otimes pb,$$

其中 $a \in A$ 和 $b \in B$．现在，如果 $\pi: A \otimes B \to (A \otimes B)/E$ 是自然映射，则

$$\hat{p}\pi = 1 \otimes p,$$

586

因为两者都把 $a \otimes b \mapsto a \otimes pb$.



假设我们证明了 $\hat{p}$ 是同构，则

$$\ker(1 \otimes p) = \ker \hat{p}\pi = \ker \pi = E = \operatorname{im}(1 \otimes i),$$

证明完成．为证明 $\hat{p}$ 确实是同构，我们构造它的逆 $A \otimes B'' \to (A \otimes B)/E$．定义

$$f: A \times B'' \to (A \otimes B)/E$$

如下．如果 $b'' \in B''$，因 p 是满射，存在 $b \in B$ 使得 $pb = b''$，设

$$f: (a, b'') \mapsto a \otimes b.$$

现在 f 是合理定义的：如果 $pb_1 = b''$，则 $p(b - b_1) = 0$ 和 $b - b_1 \in \ker p = \operatorname{im} i$. 于是存在 $b' \in B'$ 使得 $ib' = b - b_1$，因此 $a \otimes (b - b_1) = a \otimes ib' \in \operatorname{im}(1 \otimes i) = E$．显然，$f$ 是 R-双加性的，从而张量积的定义给出同态 $\hat{f}: A \otimes B'' \to (A \otimes B)/E$ 满足 $\hat{f}(a \otimes b'') = a \otimes b + E$．读者可以验证 $\hat{f}$ 就是所要的 $\hat{p}$ 的逆．

（ⅲ）$1 \otimes p$ 是满射．

如果 $\sum a_i \otimes b_i'' \in A \otimes B''$，则因 p 是满射，对一切 i 存在 $b_i \in B$ 使得 $pb_i = b_i''$. 但

$$1 \otimes p: \sum a_i \otimes b_i \mapsto \sum a_i \otimes pb_i = \sum a_i \otimes b_i''.$$ ■

对函子 $\otimes_R B$ 类似的陈述成立．如果 B 是左 R-模和

$$A' \xrightarrow{i} A \xrightarrow{p} A'' \to 0$$

是右 R-模的短正合列，则序列

$$A' \otimes_R B \xrightarrow{i \otimes 1_B} A \otimes_R B \xrightarrow{p \otimes 1_B} A'' \otimes_R B \to 0$$

是正合列．

587

定义　称（共变）函子 $T: {}_R\mathbf{Mod} \to \mathbf{Ab}$ 为**右正合的**，如果一个左 R-模序列

$$B' \xrightarrow{i} B \xrightarrow{p} B'' \to 0$$

的正合性蕴涵序列

$$T(B') \xrightarrow{T(i)} T(B) \xrightarrow{T(p)} T(B'') \to 0$$

的正合性．对共变函子 $\mathbf{Mod}_R \to \mathbf{Ab}$ 有类似的定义．

用这个术语，函子 $A \otimes_R$ 和 $\otimes_R B$ 都是右正合函子．

下面的例子解释定理 8.90 中为什么缺少"$0 \to$"．

例 8.91　考虑阿贝尔群的正合列

$$0 \to \mathbb{Z} \xrightarrow{i} \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0,$$

其中 i 是包含映射．根据右正合性，存在正合列

$$\mathrm{I}_2 \otimes \mathbb{Z} \xrightarrow{1 \otimes i} \mathrm{I}_2 \otimes \mathbb{Q} \to \mathrm{I}_2 \otimes (\mathbb{Q}/\mathbb{Z}) \to 0$$

（在这个证明中，我们把$\otimes_{\mathbb{Z}}$缩写为$\otimes$）．现在根据命题 8.86，$\mathrm{I}_2 \otimes \mathbb{Z} \cong \mathrm{I}_2$．另一方面，如果 $a \otimes q$ 是 $\mathrm{I}_2 \otimes \mathbb{Q}$ 的生成元，则

$$a \otimes q = a \otimes (2q/2) = 2a \otimes (q/2) = 0 \otimes (q/2) = 0.$$

所以，$\mathrm{I}_2 \otimes \mathbb{Q} = 0$，因此 $1 \otimes i$ 不可能是一个单射． ■

下一命题有助于张量积的计算．

命题 8.92 对每个阿贝尔群 B，有 $\mathrm{I}_n \otimes_{\mathbb{Z}} B \cong B/nB$．

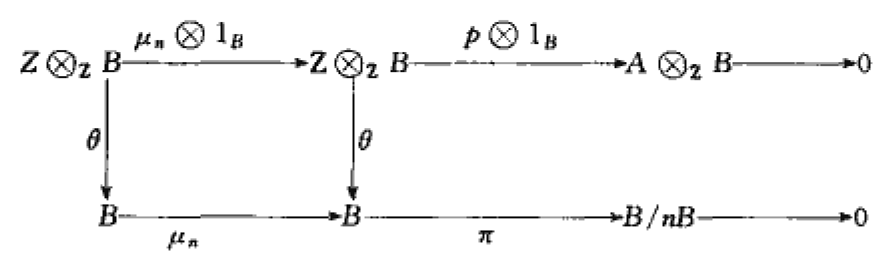
证明 如果 A 是 n 阶有限循环群，存在正合列

$$0 \to \mathbb{Z} \xrightarrow{\mu_n} \mathbb{Z} \xrightarrow{p} A \to 0,$$

其中 μ_n 是乘 n 的映射．用一个阿贝尔群 B 作张量得

$$\mathbb{Z} \otimes_{\mathbb{Z}} B \xrightarrow{\mu_n \otimes 1_B} \mathbb{Z} \otimes_{\mathbb{Z}} B \xrightarrow{p \otimes 1_B} A \otimes_{\mathbb{Z}} B \to 0$$

的正合性．考虑图



588

其中 $\theta: \mathbb{Z} \otimes_{\mathbb{Z}} B \to B$ 是命题 8.86 的同构，即 $\theta: m \otimes b \mapsto mb$，其中 $m \in \mathbb{Z}$ 和 $b \in B$. 图中两个复合都把 $m \otimes b \mapsto nmb$，所以图交换．把下一个十分广泛的命题运用到这个图上得

$$A \otimes_{\mathbb{Z}} B \cong B/nB.$$ ■

命题 8.93 给定一个行正合的交换图，其中垂直映射 f 和 g 都是同构，

$$\begin{array}{ccccccc}
A' & \xrightarrow{i} & A & \xrightarrow{p} & A'' & \longrightarrow & 0 \\
\downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \vdots{\scriptstyle h} & & \\
B' & \xrightarrow{j} & B & \xrightarrow{q} & B'' & \longrightarrow & 0
\end{array}$$

存在唯一的同构 $h: A'' \to B''$ 使得增广的图交换．

证明 如果 $a'' \in A''$，则因 p 是满射，存在 $a \in A$ 使得 $p(a) = a''$．定义 $h(a'') = qg(a)$．当然，我们必须证明 h 是合理定义的；即如果 $u \in A$ 满足 $p(u) = a''$，则 $qg(u) = qg(a)$．因 $p(a) = p(u)$，有 $p(a-u) = 0$，从而根据正合性有 $a - u \in \ker p = \operatorname{im} i$．因此有某个 $a' \in A'$ 使得 $a - u = i(a')$．于是因$qj=0$有

$$qg(a-u) = qgi(a') = qjf(a') = 0,$$

所以 h 是合理定义的．

为证明映射 h 是同构，我们构造它的逆．和第一段一样，存在映射 h' 使得下图交换：

$$\begin{array}{ccccccc}
B' & \xrightarrow{j} & B & \xrightarrow{q} & B'' & \longrightarrow & 0 \\
\downarrow{\scriptstyle f^{-1}} & & \downarrow{\scriptstyle g^{-1}} & & \vdots{\scriptstyle h'} & & \\
A' & \xrightarrow{i} & A & \xrightarrow{p} & A'' & \longrightarrow & 0
\end{array}$$

我们断言 $h' = h^{-1}$．现在 $h'q = pg^{-1}$，因此

$$h'hp = h'qg = pg^{-1}g = p;$$

因 p 是满射，有 $h'h=1_{A''}$. 类似的计算证明另一个复合 hh' 也是恒等映射．所以 h 是同构．如果 $h': A''\to B''$ 满足 $h'p=qg$，又如果 $a''\in A''$，选取 $a\in A$ 使得 $pa=a''$，则 $h'pa=h'a''=qga=ha''$，因此 h 是唯一的． ■

上面的命题的证明是**图上追踪法**的一例．这种证明虽然显得长，却是很简单的．在每一步上，选取一个元素，对于它实质上只要做一件事情．这个命题的对偶命题的证明是使用这种方法的另一例． [589]

命题 8.94　给定一个交换图，它的行是正合的，它的垂直映射是同构，

$$\begin{array}{ccccccc} 0 \longrightarrow & A' & \xrightarrow{i} & A & \xrightarrow{p} & A'' \\ & \downarrow f & & \downarrow g & & \downarrow h \\ 0 \longrightarrow & B' & \xrightarrow{j} & B & \xrightarrow{q} & B'' \end{array}$$

存在唯一的同构 $f: A'\to B'$ 使得增广的图交换．

证明　用图上追踪法． ■

两个非零模的张量积可能是零．下面的命题推广了例 8.91 中的计算．

命题 8.95　如果 T 是每个元素的阶都有限的阿贝尔群，D 是一个可除阿贝尔群，则 $T\otimes_{\mathbb{Z}} D=\{0\}$.

证明　只要证明每个生成元 $t\otimes d$ 在 $T\otimes_{\mathbb{Z}} D$ 中是 0，其中 $t\in T$ 和 $d\in D$. 因 t 的阶有限，存在非零整数 n 使得 $nt=0$. 因 D 是可除的，存在 $d'\in D$ 使得 $d=nd'$. 因此

$$t\otimes d = t\otimes nd' = nt\otimes d' = 0\otimes d' = 0.$$ ■

现在我们明白为什么不能使一个有限循环群 G 成为一个 $\mathbb{Q}$-模，这是因为 $\mathbb{Q}\otimes_{\mathbb{Z}} G=\{0\}$.

系 8.96　如果 D 是每个元素的阶都有限的非零可除阿贝尔群（例如 $D=\mathbb{Q}/\mathbb{Z}$），则没有乘法 $D\times D\to D$ 可以使 D 成为一个环．

证明　假定相反，存在乘法 $\mu: D\times D\to D$ 使 D 成为一个环．如果 1 是幺元，有 $1\neq 0$，否则 D 就是只有一个元素的零环．因环中的乘法是 $\mathbb{Z}$-双线性的，存在同态 $\tilde{\mu}: D\otimes_{\mathbb{Z}} D\to D$ 使得对一切 d, $d'\in D$ 有 $\tilde{\mu}(d\otimes d')=\mu(d,d')$. 特别地，如果 $d\neq 0$，则 $\tilde{\mu}(d\otimes 1)=\mu(d,1)=d\neq 0$. 但根据命题 8.95，$D\otimes_{\mathbb{Z}} D=\{0\}$，从而 $\tilde{\mu}(d\otimes 1)=0$. 这个矛盾表明 D 上不存在乘法 μ. ■

从 Hom 可以形成投射模和内射模，用同样的方法从张量积可以形成下面的模．在同调代数中研究 $A\otimes_R B'\to A\otimes_R B$ 的核，它和称为 Tor 的函子密切相关．

定义　如果 R 是环，则一个右 R-模称为**平坦的**[⊖]，只要

$$0\to B'\xrightarrow{i} B\xrightarrow{p} B''\to 0$$ [590]

是左 R-模的正合列，则

$$0\to A\otimes_R B'\xrightarrow{1_A\otimes i} A\otimes_R B\xrightarrow{1_A\otimes p} A\otimes_R B''\to 0$$

就是阿贝尔群的正合列．类似定义左 R-模的平坦性．

换句话说，A 是平坦的当且仅当 $A\otimes_R$ 是正合函子．因为函子 $A\otimes_R$ 是右正合的，我们知道 A 是平坦的当且仅当只要 $i: B'\to B$ 是单射，则 $1_A\otimes i: A\otimes_R B'\to A\otimes_R B$ 也是单射．

引理 8.97　如果一个右 R-模 M 的每个有限生成子模都是平坦的，则 M 是平坦模．

注　这个引理的另一个证明在系 8.103 中给出．

⊖ 把簇的几何性质翻译到代数中产生这个术语．

证明 设 $i: A \to B$ 是左 R-模之间的单射 R-映射，并假定 $u = \sum_j x_j \otimes y_j \in \ker(1_M \otimes i)$，其中 $x_j \in M$ 和 $y_j \in A$. 因 $u \in M \otimes_R A$，有

$$0 = (1_M \otimes i)u = \sum_{j=1}^{n} x_j \otimes iy_j.$$

设 F 是以 $M \times A$ 为基的自由阿贝尔群，并设 S 是由 $F/S \cong M \otimes_R A$ 的关系组成的 F 的子群（如同命题 8.74 中张量积的构造），于是 S 由 F 中形如

$$(m, a + a') - (m, a) - (m, a');$$
$$(m + m', a) - (m, a) - (m', a);$$
$$(mr, a) - (m, ra)$$

的一切元素生成. 设 M' 是 M 的子模，它由 $x_1, \cdots, x_n$ 以及把 $\sum_k (x_j, iy_j)$ 展示为刚才显示的关系子的线性组合时在 M 中的（有限个）第一个"坐标"生成. 当然，M' 是 M 的有限生成子模. 元素 $u' = \sum x_j \otimes y_j \in M' \otimes_R A$（它是 u 在这个新的张量积 $M' \otimes_R A$ 中的形式）在 $\ker 1_{M'} \otimes i$ 中，这是因为我们已经小心地使得 $(1_M \otimes i)(u) = 0$ 的一切关系仍然出现. 但 M' 是 M 的有限生成子模，从而根据假设，它是平坦的，因此 $(1_M \otimes i)(u) = 0$ 蕴涵在 $M' \otimes_R A$ 中 $u' = 0$. 最后，如果 $\ell: M' \to M$ 是包含映射，则 $(\ell \otimes 1_A)(u') = u$，从而 $u = 0$. 所以 $1_M \otimes i$ 是单射且 M 是平坦的. ■

我们将用这个引理证明一个阿贝尔群是平坦 $\mathbb{Z}$-模当且仅当没有有限阶的非零元素（见系 9.6）. 下面是平坦模的一些例子.

引理 8.98 设 R 是任意环.

591

（i）右 R-模 R 是平坦 R-模.

（ii）右 R-模的直和 $\sum_j M_j$ 是平坦的当且仅当每个 M_j 都是平坦的.

（iii）每个投射右 R-模都是平坦的.

证明 （i）考虑交换图

$$\begin{array}{ccc} A & \xrightarrow{i} & B \\ \sigma \downarrow & & \downarrow \tau \\ R \otimes_R A & \xrightarrow{1_R \otimes i} & R \otimes_R B \end{array}$$

其中 $i: A \to B$ 是单射，$\sigma: a \mapsto 1 \otimes a$ 和 $\tau: b \mapsto 1 \otimes b$. 现在根据命题 8.86，$\sigma$ 和 τ 都是同构，因此 $1_R \otimes i = \tau i \sigma^{-1}$ 是单射. 所以 R 是它自身上的平坦模.

（ii）根据命题 7.30，任一 R-映射的族 $\{f_j: U_j \to V_j\}$ 可以集中到 R-映射 $\varphi: \sum_j U_j \to \sum_j V_j$ 中，其中 $\varphi: (u_j) \mapsto (f_j(u_j))$，容易验证 φ 是单射当且仅当每个 f_j 都是单射.

设 $i: A \to B$ 是单射. 存在交换图

$$\begin{array}{ccc} \left(\sum_j M_j\right) \otimes_R A & \xrightarrow{1 \otimes i} & \left(\sum_j M_j\right) \otimes_R B \\ \downarrow & & \downarrow \\ \sum_j (M_j \otimes_R A) & \xrightarrow{\varphi} & \sum_j (M_j \otimes_R B) \end{array}$$

其中 $\varphi: (m_j \otimes a) \mapsto (m_j \otimes ia)$，1 是 $\sum_j M_j$ 上的恒等映射，向下的映射是命题 8.87 中的同构.

根据我们最初的考察，$1 \otimes i$ 是单射当且仅当每个 $1_{M_j} \otimes i$ 都是单射，这就是说 $\sum_j M_j$ 是平坦的当且仅当每个 M_j 都是平坦的．

（ⅲ）结合上面两部分，我们知道自由 R-模是 R 的复制的直和，它必定是平坦的．此外，因一个模是投射的当且仅当它是一个自由模的直和项，（ⅱ）证明投射模恒为平坦模． ■

没有进一步的假设无法改进这个引理，因为存在这样的环 R，对于它每个平坦 R-模都是投射的．

在 Hom 和 $\otimes$ 之间有一个值得注意的关系．关键的思想是二元函数，比如 $f: A \times B \to C$，可以看作一个参数的一元函数族：如果固定 $a \in A$，则定义 $f_a: B \to C$ 为 $b \mapsto f(a,b)$．回忆引理 8.80：如果 R 和 S 都是环，A_R 和 ${}_RB_S$ 是模，则 $A \otimes_R B$ 是右 S-模，其中 $(a \otimes b)s = a \otimes (bs)$．进一步，如果 C_S 是模，则易知 $\mathrm{Hom}_S(B,C)$ 是右 R-模，其中 $(fr)(b) = f(rb)$；于是 $\mathrm{Hom}_R(A, \mathrm{Hom}_S(B,C))$ 有意义，这是因为它由右 R-模之间的 R-映射组成．最后，如果 $F \in \mathrm{Hom}_R(A, \mathrm{Hom}_S(B,C))$，我们记它在 $a \in A$ 处的值为 F_a，因此由 $F_a: b \mapsto F(a)(b)$ 定义的 $F_a: B \to C$ 是一个参数的函数族． 592

定理 8.99（伴随同构） 给定模 $A_R, {}_RB_S$ 和 C_S，其中 R 和 S 都是环，存在同构

$$\tau_{A,B,C}: \mathrm{Hom}_S(A \otimes_R B, C) \to \mathrm{Hom}_R(A, \mathrm{Hom}_S(B,C)),$$

即对 $f: A \otimes_R B \to C$ 和 $a \in A, b \in B$，

$$\tau_{A,B,C}: f \mapsto f^*，\text{其中 } f_a^*: b \mapsto f(a \otimes b).$$

事实上，固定 A,B,C 中的任意两个，映射 $\tau_{A,B,C}$ 构成自然等价

$$\mathrm{Hom}_S(\ \otimes_R B, C) \to \mathrm{Hom}_R(\ , \mathrm{Hom}_S(B,C)),$$
$$\mathrm{Hom}_S(A \otimes_R\ , C) \to \mathrm{Hom}_R(A, \mathrm{Hom}_S(\ , C))$$

和

$$\mathrm{Hom}_S(A \otimes_R B,\ ) \to \mathrm{Hom}_R(A, \mathrm{Hom}_S(B,\ )).$$

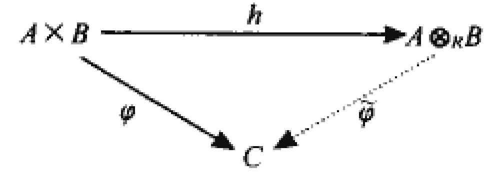
证明 为证明 $\tau = \tau_{A,B,C}$ 是 $\mathbb{Z}$-同态，设 $f, g: A \otimes_R B \to C$. $f+g$ 的定义给出对一切 $a \in A$，

$$\tau(f+g)_a: b \mapsto (f+g)(a \otimes b) = f(a \otimes b) + g(a \otimes b)$$
$$= \tau(f)_a(b) + \tau(g)_a(b).$$

所以 $\tau(f+g) = \tau(f) + \tau(g)$．

其次，τ 是单射．如果对一切 $a \in A, \tau(f_a) = 0$，则对一切 $a \in A$ 和 $b \in B$，$0 = \tau(f)_a(b) = f(a \otimes b)$．因为 f 把 $A \otimes_R B$ 的每个生成元变成 0，所以 $f = 0$.

现在证明 τ 是满射．如果 $F: A \to \mathrm{Hom}_S(B,C)$ 是 R-映射，定义 $\varphi: A \times B \to C$ 为 $\varphi(a,b) = F_a(b)$．考虑图



容易验证 φ 是 R-双加性的，因此存在 $\mathbb{Z}$-同态 $\tilde{\varphi}: A \otimes_R B \to C$ 使得对一切 $a \in A$ 和 $b \in B$，$\tilde{\varphi}(a \otimes b) = \varphi(a,b) = F_a(b)$．所以 $F = \tau(\tilde{\varphi})$，从而 τ 是满射．

我们让读者证明命题指定的映射是自然变换，要求给出图及其交换性的证明． ■

给定任意两个函子 $F: \mathcal{C} \to \mathcal{D}$ 和 $G: \mathcal{D} \to \mathcal{C}$，称有序对 (F,G) 为**伴随对**，如果对每个对象 $C \in \mathcal{C}$ 和 $D \in \mathcal{D}$ 的对，存在双射

$$\tau_{C,D}: \mathrm{Hom}_{\mathcal{D}}(FC, D) \to \mathrm{Hom}_{\mathcal{C}}(C, GD),$$

[593] 它们是 C 和 D 中的自然变换．根据定理 8.99，$(\ \otimes_R B, \mathrm{Hom}(B,\ ))$ 是一个伴随对．

如早先的承诺，这里是定理 8.90——张量积的右正合性——的另一个证明．因 $(\ \otimes_R B, \mathrm{Hom}(B,\ ))$ 是函子的伴随对，根据定理 7.105，右函子 $\otimes$ 必保持一切正向极限．但余核是正向极限，而一个函子如果保持余核则是右正合的．下面是具体的证明．

命题 8.100 *设 A 是右 R-模，并设*

$$B' \xrightarrow{i} B \xrightarrow{p} B'' \to 0$$

是左 R-模的正合列，则

$$A \otimes_R B' \xrightarrow{1_A \otimes i} A \otimes_R B \xrightarrow{1_A \otimes p} A \otimes_R B'' \to 0$$

是阿贝尔群的正合列．

证明 把左 R-模 B 看作 $(R,\mathbb{Z})$-双模，并注意，根据习题 8.45，对任意阿贝尔群 C，$\mathrm{Hom}_{\mathbb{Z}}(B,C)$ 是右 R-模．依据命题 7.48，只要证明对每个 C，下图的顶上一行是正合的：

$$\begin{array}{ccccccc}
0 \to & \mathrm{Hom}_{\mathbb{Z}}(A \otimes_R B'', C) & \to & \mathrm{Hom}_{\mathbb{Z}}(A \otimes_R B, C) & \to & \mathrm{Hom}_{\mathbb{Z}}(A \otimes_R B', C) \\
& \downarrow \tau''_{A,C} & & \downarrow \tau_{A,C} & & \downarrow \tau'_{A,C} \\
0 \to & \mathrm{Hom}_R(A, H'') & \to & \mathrm{Hom}_R(A, H) & \to & \mathrm{Hom}_R(A, H')
\end{array}$$

其中 $H'' = \mathrm{Hom}_{\mathbb{Z}}(B'',C)$，$H = \mathrm{Hom}_{\mathbb{Z}}(B,C)$，$H' = \mathrm{Hom}_{\mathbb{Z}}(B',C)$．根据伴随同构，垂直映射是同构且图交换．因为底下的一行是对给定的正合列 $B' \to B \to B'' \to 0$ 先用左正合（反变）函子 $\mathrm{Hom}_{\mathbb{Z}}(\ ,C)$ 作用、再用左正合（共变）函子 $\mathrm{Hom}_R(A,\ )$ 作用得到的，所以它是正合的．现在顶上一行的正合性由习题 8.51 得到． ■

在定理 7.92 中，我们证明了 $\mathrm{Hom}(A,\ )$ 保持反向极限，现在证明 $A\otimes$ 保持正向极限．这也可以从定理 7.105 得到．然而，我们给出基于正向极限构造的另一个证明．

定理 8.101 *如果 A 是右 R-模，$\{B_i, \varphi_j^i\}$ 是左 R-模的正系统（在任意的、不必有向的指标集 I 上），则*

$$A \otimes_R \varinjlim B_i \cong \varinjlim (A \otimes_R B_i).$$

证明 注意习题 7.66 证明 $\{A \otimes_R B_i, 1 \otimes \varphi_j^i\}$ 是正系统，从而 $\varinjlim (A \otimes_R B_i)$ 有意义．我们先把 $\varinjlim B_i$ 作为和之间的某个映射的余核来构造．对偏序指标集 I 中满足 $i \preceq j$ 的每对 $i, j \in I$，定义 B_{ij} 为经映射 $b_i \mapsto b_{ij}$ 而同构于 B_i 的模，其中 $b_i \in B_i$，并定义 $\sigma: \sum_{ij} B_{ij} \to \sum_i B_i$ 为

[594]

$$\sigma: b_i \mapsto \lambda_j \varphi_j^i b_i - \lambda_i b_i,$$

其中 λ_i 是 B_i 到和的内射．注意 $\mathrm{im}\sigma = S$，S 是命题 7.94 中构造 $\varinjlim B_i$ 形成的子模．于是，$\mathrm{coker}\sigma = (\sum B_i)/S \cong \varinjlim B_i$，且存在正合列

$$\sum B_{ij} \xrightarrow{\sigma} \sum B_i \to \varinjlim B_i \to 0.$$

$A \otimes_R$ 的右正合性给出

$$A \otimes_R (\sum B_{ij}) \xrightarrow{1 \otimes \sigma} A \otimes_R (\sum B_i) \to A \otimes_R (\varinjlim B_i) \to 0$$

的正合性．

根据定理 8.87，由

$$\tau: a \otimes (b_i) \mapsto (a \otimes b_i)$$

给出的映射 $\tau: A\otimes_R(\sum_i B_i)\to\sum_i(A\otimes_R B_i)$ 是同构，因此存在交换图

$$\begin{array}{ccccccc} A\otimes\sum B_{ij} & \xrightarrow{1\otimes\sigma} & A\otimes\sum B_i & \longrightarrow & A\otimes\varinjlim B_i & \longrightarrow & 0\\ \downarrow{\scriptstyle\tau} & & \downarrow{\scriptstyle\tau'} & & \vdots & & \\ \sum(A\otimes B_{ij}) & \xrightarrow{\widetilde{\sigma}} & \sum(A\otimes B_i) & \longrightarrow & \varinjlim(A\otimes B_i) & \longrightarrow & 0 \end{array}$$

其中 τ'是定理 8.87 的同构的另一例，且

$$\widetilde{\sigma}: a\otimes b_{ij}\mapsto(1\otimes\lambda_j)(a\otimes\varphi_j^i b_i)-(1\otimes\lambda_i)(a'\otimes b_i).$$

根据命题 8.93，存在同构 $A\otimes_R\varinjlim B_i\to\operatorname{coker}\widetilde{\sigma}\cong\varinjlim(A\otimes_R B_i)$，即正系统 $\{A\otimes_R B_i, 1\otimes\varphi_j^i\}$ 的正向极限． ■

读者或许观察到事实上我们已经证明了更强的结果：保持和的任一右正合函子必保持一切正向极限．对偶的结果也成立，证明也类似：保持积的每个左正合函子必保持一切反向极限．事实上，如果 (F,G) 是（定义在模范畴上的）函子的伴随对，则 F 保持正向极限，G 保持反向极限．

系 8.102　*如果 $\{F_i,\varphi_j^i\}$ 是有向指标集 I 上的平坦右 R-模的正系统，则 $\varinjlim F_i$ 也是平坦的．*

证明　设 $0\to A\xrightarrow{k}B$ 是左 R-模的正合列．因每个 F_i 都是平坦的，序列

$$0\to F_i\otimes_R A\xrightarrow{1_i\otimes k}F_i\otimes_R B$$

对每个 i 都是正合的，其中 1_i 是 1_{F_i} 的缩写．考虑交换图

$$\begin{array}{ccccc} 0\longrightarrow & \varinjlim(F_i\otimes A) & \xrightarrow{\vec{k}} & \varinjlim(F_i\otimes B) \\ & \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle\psi} \\ 0\longrightarrow & (\varinjlim F_i)\otimes A & \xleftarrow{1\otimes k} & (\varinjlim F_i)\otimes B \end{array}$$

595

其中垂直映射 φ 和ψ是定理 8.101 的同构，映射 $\vec{k}$ 是从正系统 $\{1_i,\otimes k\}$ 的变换导出的，1 是$\varinjlim F_i$ 上的恒等映射．因每个 F_i 都是平坦的，所以映射 $1_i\otimes k$ 是单射；因指标集 I 是有向的，根据命题 7.100，顶上一行是正合的．所以 $1\otimes k:(\varinjlim F_i)\otimes A\to(\varinjlim F_i)\otimes B$ 是单射，这是因为它是单射的复合 $\psi\vec{k}\varphi^{-1}$．所以$\varinjlim F_i$ 是平坦的． ■

系 8.103　（ⅰ）*如果 R 是整环，且 $Q=\operatorname{Frac}(R)$，则 Q 是平坦 R-模．*

（ⅱ）*如果右 R-模 M 的每个有限生成子模都是平坦的，则 M 是平坦的．*

证明　（ⅰ）在例7.97(ⅴ)中，我们看到 Q 是一个有向指标集上每个都同构于 R 的循环子模的正向极限．因 R 是投射的，因此是平坦的，从系 8.102 可得结果．

（ⅱ）在例7.99(ⅲ)中，我们看到 M 是一个有向指标集上 M 的有限生成子模的正向极限．因为根据假设，每个有限生成子模是平坦的，所以从系 8.102 可得结果．我们已经给出引理 8.97 的另一个证明． ■

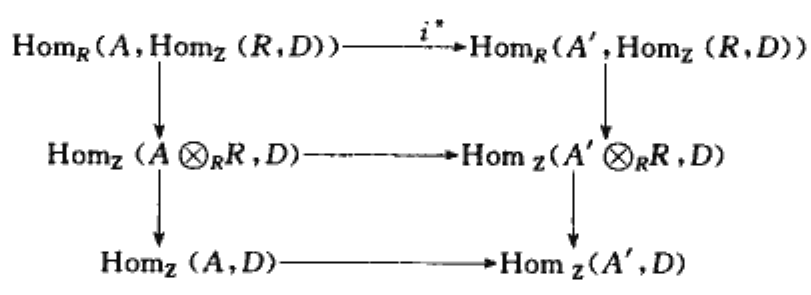
系 7.75 可以从阿贝尔群扩张到任意环上的模．

定理 8.104　*对每个环 R，每个左 R-模 M 能够作为子模嵌入一个内射左 R-模．*

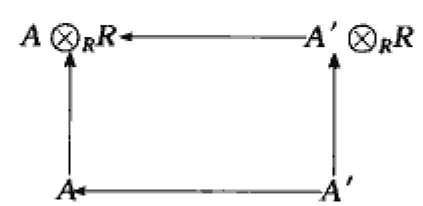
证明　把 R 看作双模$_{\mathbb{Z}}R_R$，并把一个阿贝尔群 D 看作一个左 $\mathbb{Z}$-模，我们用习题 8.45 来证明 $\operatorname{Hom}_{\mathbb{Z}}(R,D)$是左 R-模；标量乘法 $R\times\operatorname{Hom}_{\mathbb{Z}}(R,D)\to\operatorname{Hom}_{\mathbb{Z}}(R,D)$ 由 $(a,\varphi)\mapsto a\varphi$ 给出，其中

$a\varphi: r \mapsto \varphi(ra)$.

现在如果 D 是可除阿贝尔群，我们断言 $H = \mathrm{Hom}_{\mathbb{Z}}(R,D)$ 是内射 R-模，即可以证明 $\mathrm{Hom}_R(\ ,H)$ 是正合函子．因 Hom 是左正合的，只需证明如果 $i: A' \to A$ 是单射，则诱导映射 $i^*: \mathrm{Hom}_R(A,H) \to \mathrm{Hom}_R(A',H)$ 是满射．考虑下面的图．



596 伴随同构给出顶上一个方形的交换性．底下一个方形是用反变函子 $\mathrm{Hom}_{\mathbb{Z}}(\ ,D)$ 作用到下面的图得到的：



因为由 $a \mapsto a \otimes 1$ 给出的同构 $A \to A \otimes_R R$ 是自然映射，所以该图交换．因 D 是可除的，系 7.73 说 D 是内射$\mathbb{Z}$-模．所以 $\mathrm{Hom}_{\mathbb{Z}}(\ ,D)$ 是正合函子，且大图的底下一行是满射．因大图中的一切垂直映射都是同构，现在交换性给出 i^* 是满射．由此推出 $\mathrm{Hom}_{\mathbb{Z}}(R,D)$是内射左 R-模．

最后，把 M 看作阿贝尔群．根据系 7.75，存在可除阿贝尔群 D 和单射$\mathbb{Z}$-同态 $j: M \to D$．现在易知存在单射 R-映射 $M \to \mathrm{Hom}_{\mathbb{Z}}(R,D)$，就是 $m \mapsto f_m$，其中 $f_m(r) = j(rm) \in D$，证明完成． ■

因为存在包含任意给定的模的最小内射模（称为**内射包络**），因此上面的定理可以进一步改进（见 Rotman 所著的《An Introduction to Homological Algebra》，73 页）．

在命题 7.69 中我们已经看到，如果 R 是诺特环，则内射模的每个直和也是内射模．我们现在证明逆命题．

定理 8.105（巴斯） *如果 R 是环，对于它每个内射左 R-模的直和也是内射模，则 R 是左诺特环．*

证明 我们证明如果 R 不是左诺特环，则存在左理想 I 以及一个到内射模之和的 R-映射，而这个映射不能扩张到 R. 因 R 不是左诺特环，存在左理想的严格升链 $I_1 \subsetneq I_2 \subsetneq \cdots$；令 $I = \bigcup I_n$．注意对一切 $n, I/I_n \neq \{0\}$．根据定理 8.104，可以把 I/I_n 嵌入一个内射左 R-模 E_n；我们断言 $E = \sum_n E_n$ 不是内射模．

设 $\pi_n: I \to I/I_n$ 是自然映射．对每个 $a \in I$，注意对大的 n 有 $\pi_n(a) = 0$（因为有某个 n 使得 $a \in I_n$），因此由

$$f: a \mapsto (\pi_n(a))$$

定义的 R-映射 $f: I \to \prod (I/I_n)$的象在 $\sum_n (I/I_n)$ 中；即对 $a \in I$，$f(a)$的一切坐标几乎都等于 0. 与包含映射$\sum(I/I_n) \to \sum E_n = E$ 结合，可以把 f 看作映射 $I \to E$. 如果存在扩张 f 的 R-映射 $g: R \to E$，则 $g(1)$ 有定义，比如 $g(1) = (x_n)$．选取一个指标 m 并选取 $a \in I$ 而 $a \notin I_m$；因 $a \notin I_m$，有 $\pi_m(a) \neq 0$，从而 $g(a) = f(a)$ 的第 m 个坐标 $\pi_m(a)$ 非零．但 $g(a) = ag(1) = a(x_n) = (ax_n)$，因此 $\pi_m(a) = ax_m$. 由此对一切 m，$x_m \neq 0$，这与 $g(1)$ 在直和 $E = \sum E_n$ 中矛盾． ■

我们现在给出平坦模和投射模之间的联系．

597

定义　如果 B 是右 R-模，定义它的**特征标模** B^* 为左 R-模

$$B^* = \mathrm{Hom}_{\mathbb{Z}}(B, \mathbb{Q}/\mathbb{Z}).$$

回忆如果对 $r \in R$ 和 $f: B \to \mathbb{Q}/\mathbb{Z}$ 定义 rf 为

$$rf: b \mapsto f(br),$$

则 B^* 是左 R-模．

下一引理改进了命题 7.48：如果 $i: A' \to A$ 和 $p: A \to A''$ 都是映射，且对每个模 B，

$$0 \to \mathrm{Hom}(A'', B) \xrightarrow{p^*} \mathrm{Hom}(A, B) \xrightarrow{i^*} \mathrm{Hom}(A', B)$$

是正合列，则

$$A' \xrightarrow{i} A \xrightarrow{p} A'' \to 0$$

也是正合列．

引理 8.106　*一个右 R-模的序列*

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

是正合的当且仅当特征标模的序列

$$0 \to C^* \xrightarrow{\beta^*} B^* \xrightarrow{\alpha^*} A^* \to 0$$

是正合的．

证明　如果原始序列是正合的，则因反变函子 $\mathrm{Hom}_{\mathbb{Z}}(\ ,\mathbb{Q}/\mathbb{Z})$ 是正合的，所以特征标模序列也是正合的，而反变函子 $\mathrm{Hom}_{\mathbb{Z}}(\ ,\mathbb{Q}/\mathbb{Z})$ 的正合性是根据系 7.73，因为 $\mathbb{Q}/\mathbb{Z}$ 是内射 $\mathbb{Z}$-模．

对于逆命题，只要证明 $\mathrm{im}\alpha = \ker\beta$，而不用假定 α^* 是满射或 β^* 是单射．

$\mathrm{im}\alpha \subseteq \ker\beta$．如果 $x \in A$ 和 $\alpha x \notin \ker\beta$，则 $\beta\alpha(x) \neq 0$．根据习题 7.57 (i)，存在映射 $f: C \to \mathbb{Q}/\mathbb{Z}$ 使得 $f\beta\alpha(x) \neq 0$．于是 $f \in C^*$ 且 $f\beta\alpha \neq 0$，与假设 $\alpha^*\beta^* = 0$ 矛盾．

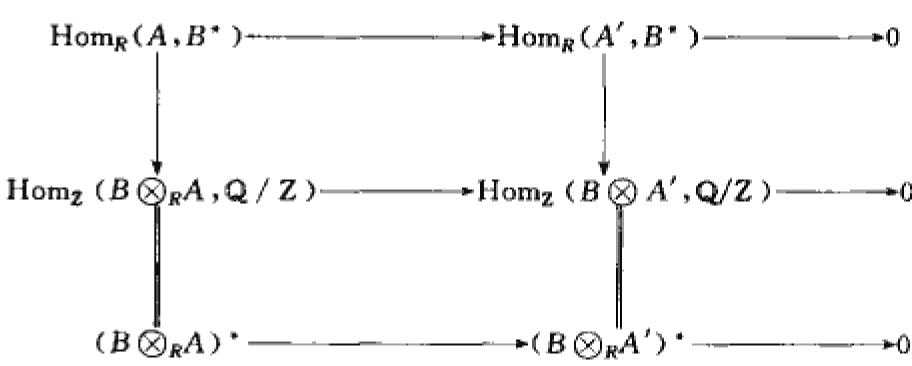
$\ker\beta \subseteq \mathrm{im}\alpha$．如果 $y \in \ker\beta$ 和 $y \notin \mathrm{im}\alpha$，则 $y + \mathrm{im}\alpha$ 是 $B/\mathrm{im}\alpha$ 的非零元素．于是根据习题 7.57 (i)，存在映射 $g: B/\mathrm{im}\alpha \to \mathbb{Q}/\mathbb{Z}$ 使得 $g(y + \mathrm{im}\alpha) \neq 0$．如果 $v: B \to B/\mathrm{im}\alpha$ 是自然映射，定义 $g' = gv \in B^*$；注意，因为 $g'(y) = gv(y) = g(y + \mathrm{im}\alpha)$，所以 $g'(y) \neq 0$．现在 $g'(\mathrm{im}\alpha) = \{0\}$，从而 $0 = g'\alpha = \alpha^*(g')$ 和 $g' \in \ker\alpha^* = \mathrm{im}\beta^*$．于是有某个 $h \in C^*$ 使得 $g' = \beta^*(h)$；即 $g' = h\beta$．因此 $g'(y) = h\beta(y)$，这是一个矛盾，因为 $g'(y) \neq 0$，而因 $y \in \ker\beta$，有 $h\beta(y) = 0$．　■

598

命题 8.107　*右 R-模 B 是平坦的当且仅当它的特征标模 B^* 是内射左 R-模．*

证明　在定理 8.104 的证明中让 B 扮演 R 的角色（由此，平坦性蕴涵映射 $A' \otimes_R B \to A \otimes_R B$ 是单射），则左 R-模 $B^* = \mathrm{Hom}_{\mathbb{Z}}(B, \mathbb{Q}/\mathbb{Z})$ 是内射模．

反之，假定 B^* 是内射左 R-模和 $A' \to A$ 是左 R-模 A' 和 A 之间的单射．因 $\mathrm{Hom}_R(A, B^*) = \mathrm{Hom}_R(A, \mathrm{Hom}_{\mathbb{Z}}(B, \mathbb{Q}/\mathbb{Z}))$，伴随同构，即定理 8.99 给出交换图，其中垂直映射是同构．



现在顶上一行的正合性给出底下一行的正合性．根据引理 8.106，序列 $0 \to B \otimes_R A' \to B \otimes_R A$ 是正合的，由此，B 是平坦的． ■

系 8.108 *右 R-模 B 是平坦的当且仅当对每个有限生成左理想 I，序列 $0 \to B \otimes_R I \to B \otimes_R R$ 是正合的．*

证明 如果 B 是平坦的，则对每个左 R-模 I，序列 $0 \to B \otimes_R I \to B \otimes_R R$ 是正合的；特别是当 I 是有限生成左理想时，这个序列是正合的．反之，对每个有限生成左理想 I，序列 $0 \to B \otimes_R I \to B \otimes_R R$ 的正合性假设使得可以用命题 7.100 和张量积与正向极限可交换的事实，对每个左理想证明该序列的正合性．根据伴随同构，有正合列 $(B \otimes_R R)^* \to (B \otimes_R I)^* \to 0$，它给出 $\mathrm{Hom}_R(R, B^*) \to \mathrm{Hom}_R(I, B^*) \to 0$ 的正合性．这就是说从一个理想 I 到 B^* 的每个映射可以扩张为映射 $R \to B^*$；于是 B^* 满足白尔判别法，即定理 7.68，从而 B^* 是内射的．根据命题 8.107，B 是平坦的． ■

引理 8.109 *给定模 $({}_RX, {}_RY_S, Z_S)$，其中 R 和 S 都是环，存在 X，Y 和 Z 中的自然变换*

$$\tau_{X,Y,Z} : \mathrm{Hom}_S(Y, Z) \otimes_R X \to \mathrm{Hom}_S(\mathrm{Hom}_R(X, Y), Z).$$

此外，当 X 是有限生成自由左 R-模时，$\tau_{X,Y,Z}$ 是同构．

证明 注意，因为 Y 是双模，所以 $\mathrm{Hom}_S(Y,Z)$ 和 $\mathrm{Hom}_R(X,Y)$ 都有意义．如果 $f \in \mathrm{Hom}_S(Y, Z)$ 和 $x \in X$，定义 $\tau_{X,Y,Z}(f \otimes x)$ 为由

[599]

$$\tau_{X,Y,Z}(f \otimes x) : g \mapsto f(g(x))$$

给出的 S-映射 $\mathrm{Hom}_R(X,Y) \to Z$.

容易验证 $\tau_{X,Y,Z}$ 是 X 中的自然同态，$\tau_{R,Y,Z}$ 是同构，以及更一般地，当 X 是有限生成的自由左 R-模时，$\tau_{X,Y,Z}$ 是同构． ■

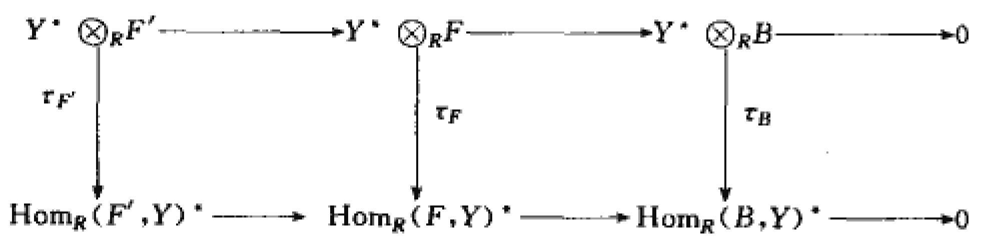
定理 8.110 *有限表现的左 R-模 B 是平坦模当且仅当它是投射模．*

证明 根据引理 8.98，一切投射模都是平坦的，所以只有逆命题是值得注意的．因 B 是有限表现的，存在正合列

$$F' \to F \to B \to 0,$$

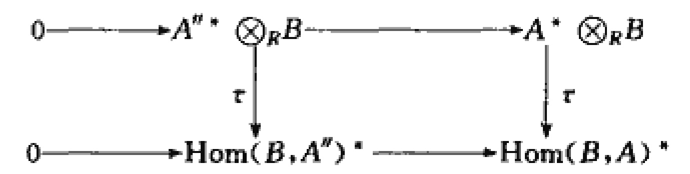
其中 F' 和 F 都是有限生成的自由左 R-模．我们先证明对每个左 R-模 Y[它必定是 $(R,\mathbb{Z})$-双模]，引理 8.109 中的映射 $\tau_B = \tau_{B,Y,\mathbb{Q}/\mathbb{Z}} : Y^* \otimes_R B \to \mathrm{Hom}_R(B,Y)^*$ 是同构．

考虑下面的图．



根据引理 8.109，该图交换 [因为 $Y^* \otimes_R F = \mathrm{Hom}_\mathbb{Z}(Y, \mathbb{Q}/\mathbb{Z}) \otimes_R F$] 且前面两个垂直映射是同构．现在因为 $Y^* \otimes_R$ 是右正合的，所以顶上一行是正合的．因为 $\mathrm{Hom}_R(\ ,Y)^*$ 是左正合的反变函子 $\mathrm{Hom}_R(\ ,Y)$ 和正合的 $^* = \mathrm{Hom}_\mathbb{Z}(\ ,\mathbb{Q}/\mathbb{Z})$ 的复合，所以底下一行也是正合的．现在命题 8.93 表明第三个垂直箭头 $\tau_B : Y^* \otimes_R B \to \mathrm{Hom}_R(B,Y)^*$ 是同构．

为证明 B 是投射的，只要证明 $\mathrm{Hom}(B,\ )$ 保持满射：如果 $A \to A'' \to 0$ 是正合的，则 $\mathrm{Hom}(B,A) \to \mathrm{Hom}(B,A'') \to 0$ 是正合的．根据引理 8.106，只要证明 $0 \to \mathrm{Hom}(B,A'')^* \to \mathrm{Hom}(B,A)^*$ 是正合的．考虑图



τ的自然性给出图的交换性，而因B是有限表现的，所以垂直映射τ是同构．因$A\to A''\to 0$是正合的，所以$0\to A''^{*}\to A^{*}$是正合的，又因B是平坦的，所以顶上一行是正合的．由此底下一行也是正合的；即$0\to \mathrm{Hom}(B,A'')^{*}\to \mathrm{Hom}(B,A)^{*}$是正合的，这就是我们所要证明的．所以$B$是投射模． ■ 600

系 8.111 如果R是右诺特环，则一个有限生成右R-模是平坦的当且仅当它是投射模．

证明 回忆命题 7.59（它对非交换环成立）：一个诺特环上的每个有限生成模都是有限表现的．由此该结果立刻从定理得到． ■

下面是张量积的一个好的应用，它帮助我们把韦德伯恩-阿廷定理摆到一个正确的位置上．

定义 一个模P称为小的，如果共变 Hom 函子$\mathrm{Hom}(P,\ )$保持（可以无限）直和．

例如，命题 8.85 证明每个环R都是小R-模．

说P是小的不仅意味着存在某个同构

$$\mathrm{Hom}\Big(P,\sum_{i\in I}B_i\Big)\cong\sum_{i\in I}\mathrm{Hom}(P,B_i);$$

也意味着$\mathrm{Hom}(P,\ )$保持余积图；如果$\lambda_i:B_i\to B$是内射，其中$B=\sum_{i\in I}B_i$，则诱导映射$(\lambda_i)^{*}$：$\mathrm{Hom}(P,B_i)\to\mathrm{Hom}(P,B)$是$\sum_{i\in I}\mathrm{Hom}(P,B_i)$的内射．

例 8.112 （i）小模的任意有限直和也是小模，一个小模的任意直和项也是小模．

（ii）因环R是小R-模，由此根据（i），每个有限生成自由R-模是小模，且每个有限生成投射R-模是小模． ■

定义 一个右R-模P称为$\mathbf{Mod}_R$的生成元，如果每个右R-模M都是P的复制的某个直和的商

显然，和任意自由右R-模一样．R是$\mathbf{Mod}_R$的生成元．然而，一个投射右R-模可以不是生成元．例如，如果$R=\mathbb{I}_6$，则$R=P\otimes Q$，其中$P=\{[0],[2],[4]\}\cong\mathbb{I}_3$，投射模$P$不是生成元（因为$Q\cong\mathbb{I}_2$不是$P$的复制的直和的商）．

定理 8.113 设R是环，并设P是$\mathbf{Mod}_R$的一个小投射生成元．如果$S=\mathrm{End}_R(P)$，则存在范畴的等价

$$\mathbf{Mod}_R\cong\mathbf{Mod}_S.$$

证明 注意，如果$x\in P$和f，$g\in S=\mathrm{End}_R(P)$，则$(g\circ f)x=g(fx)$，所以P是左S-模．事实上，P是(S,R)-双模，这是因为结合性$f(xr)=(fx)r$，其中$r\in R$，就是说明f是R-映射．现在由系 8.81，定义为$F=\ \otimes_S P$的函子$F:\mathbf{Mod}_S\to\mathbf{Ab}$实际上在$\mathbf{Mod}_R$中取值．习题 8.45（ii）证明函子$G:\mathrm{Hom}_R(P,\ ):\mathbf{Mod}_R\to\mathbf{Ab}$实际上在$\mathbf{Mod}_S$中取值．因为$(F,G)$是伴随对，习题 7.75 给出自然变换$FG\to 1_R$和$1_S\to GF$，其中$1_R$和$1_S$分别表示范畴$\mathbf{Mod}_R$和$\mathbf{Mod}_S$上的单位函子．只需证明这两个自然变换都是自然等价． 601

因P是投射右R-模，函子$G=\mathrm{Hom}_R(P,\ )$是正合的；因P是小模，G保持直和．现在$F=\ \otimes_S P$和任意张量积函子一样是右正合的并保持和．所以，复合GF和FG都保持直和，且都是右正合的．

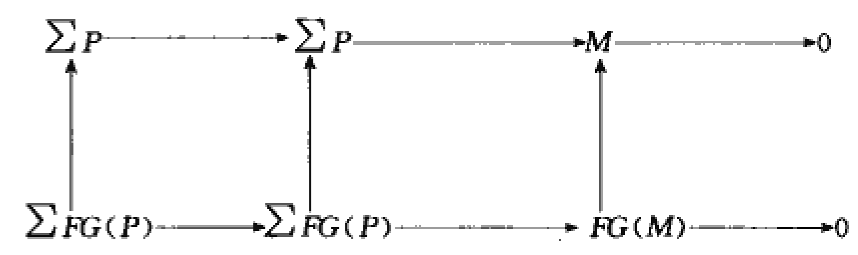
注意

$$FG(P) = F(\mathrm{Hom}_R(P,P)) = F(S) = S \otimes_S P \cong P.$$

因 P 是 $\mathbf{Mod}_R$ 的生成元，每个右 R-模都是 P 的复制的某个直和的商：存在正合列 $K \to \sum P \xrightarrow{f} M \to 0$，其中 $K = \ker f$. 还存在 P 的复制的某个直和映射到 K 上，从而有正合列

$$\sum P \to \sum P \to M \to 0.$$

因此，存在行正合的交换图（由向上映射的自然性）



我们知道前两个垂直映射是同构，从而图上追踪法（见习题 8.52 的五引理）给出另一垂直映射也是同构；即 $FG(M) \cong M$，因此 $1_R \cong FG$.

对于另一个复合，注意

$$GF(S) = G(S \otimes_S P) \cong G(P) = \mathrm{Hom}_R(P,P) = S.$$

如果 N 是左 S-模，存在形如

$$\sum S \to \sum S \to N \to 0$$

的正合列，这是因为每个模都是自由模的商．现在结论可如刚才做的那样推出． ■

系 8.114 如果 R 是环且 $n \geqslant 1$，存在范畴的等价

$$\mathbf{Mod}_R \cong \mathbf{Mod}_{\mathrm{Mat}_n(R)}.$$

602

注 根据习题 8.22，存在范畴的等价 ${}_{R^{\mathrm{op}}}\mathbf{Mod} \to \mathbf{Mod}_R$. 特别地，如果 R 是交换环，则

$${}_R\mathbf{Mod} \cong \mathbf{Mod}_{\mathrm{Mat}_n(R)}.$$

证明 对任意整数 $n \geqslant 1$，自由模 $P = \sum_{i=1}^{n} R_i$（其中 $R_i \cong R$）是 $\mathbf{Mod}_R$ 的小投射生成元，且 $S = \mathrm{End}_R(P) \cong \mathrm{Mat}_n(R)$． ■

现在我们可以理解命题 8.49：当 Δ 是除环时，$\mathrm{Mat}_n(\Delta)$ 是半单的．根据命题 8.48，环 R 是半单的当且仅当每个 R-模都是投射的；即 $\mathbf{Mod}_R$ 中的每个对象都是投射的．现在每个 Δ-模是投射的（甚至是自由的），因此范畴的等价表明 $\mathbf{Mod}_{\mathrm{Mat}_n(\Delta)}$ 中的每个对象也是投射的．所以，$\mathrm{Mat}_n(\Delta)$ 也是半单的．

有一个思想派系，通常叫做**森田理论**（以森田命名）．第一个问题是问什么时候一个抽象的范畴$\mathcal{C}$等价于 $\mathbf{Mod}_R$，其中 R 是某个环．答案是十分完美的：一个范畴$\mathcal{C}$同构于一个模范畴当且仅当它是一个**阿贝尔范畴**（这正好说明第 7.2 节中通常的有限构造存在；见 Mac Lane 所著的《Categories for the Working Mathematician》，187～206 页），它在无限余积下封闭，并且它包含一个小投射对象 P 作为生成元．给出这些假设，则 $\mathcal{C} \cong \mathbf{Mod}_S$，其中 $S = \mathrm{End}(P)$（它的证明本质上是对定理 8.113 给出的证明）．

两个环 R 和 S 称为**森田等价**，如果 $\mathbf{Mod}_R \cong \mathbf{Mod}_S$. 例如由定理 8.113，每个交换环 R 森田等价于环 $\mathrm{Mat}_n(R)$，其中 $n \geqslant 1$. 此外，如果 R 和 S 是森田等价的，则 $Z(R) \cong Z(S)$；即它们有同构的中心（它的证明实际上是识别范畴间一切可能的同构）．特别地，两个交换环是森田等价的当且仅当它们同构．见 Jacobson 所著的《Basic Algebra Ⅱ》177～184 页，Lam 所著的《Lectures on Modules and Rings》第 18～19 章，以及 Reiner 所著的《Maximal Orders》第 4 章．

下一章中，我们会看到两个 k-代数 R 和 S 的张量积 $R\otimes_k S$ 也是 k-代数．确实，当 R 和 S 都是交换代数时，$R\otimes_k S$ 是它们在交换 k-代数范畴中的余积．

习题

8.45 这个习题类似于系 8.81.

(i) 给定双模 ${}_RA_S$，证明 $\mathrm{Hom}_R(A,\ ):{}_R\mathbf{Mod}\to{}_S\mathbf{Mod}$ 是函子，其中 $\mathrm{Hom}_R(A,B)$ 是由 $sf: a\mapsto f(as)$ 定义的左 S-模．

(ii) 给定双模 ${}_RA_S$，证明 $\mathrm{Hom}_S(A,\ ):\mathbf{Mod}_S\to\mathbf{Mod}_R$ 是函子，其中 $\mathrm{Hom}_S(A,B)$ 是由 $fr: a\mapsto f(ra)$ 定义的右 R-模．

(iii) 给定双模 ${}_SB_R$，证明 $\mathrm{Hom}_R(\ ,B):\mathbf{Mod}_R\to{}_S\mathbf{Mod}$ 是函子，其中 $\mathrm{Hom}_R(A,B)$ 是由 $sf: a\mapsto s[f(a)]$ 定义的左 S-模．

(iv) 给定双模 ${}_SB_R$，证明 $\mathrm{Hom}_S(A,\ ):{}_S\mathbf{Mod}\to\mathbf{Mod}_R$ 是函子，其中 $\mathrm{Hom}_S(A,B)$ 是由 $fr: a\mapsto f(a)r$ 定义的右 R-模．

603

注：设 $f: A\to B$ 是 R-映射．假设当 A 是右 R-模时，我们写作 $f(a)$，当 A 是左 R-模时，我们写作 $(a)f$（即把函数符号 f 写在标量作用的另一面）．用这个记号，本习题的四个部分都是一个结合律．例如，在（i）中，A 和 B 都是左 R-模，对 $s\in S$ 写作 sf，我们有 $a(sf)=(as)f$．同样，在（ii）中，对 $r\in R$，我们定义 fr，从而 $(fr)a=f(ra)$．

8.46 设 V 和 W 都是域 k 上的有限维向量空间，比如设 $v_1,\cdots,v_m$ 和 $w_1,\cdots,w_n$ 分别是 V 和 W 的基．设 $S: V\to V$ 是有矩阵 $A=[a_{ij}]$ 的线性变换，$T: W\to W$ 是有矩阵 $B=[b_{k\ell}]$ 的线性变换．证明 $S\otimes T: V\otimes_k W\to V\otimes_k W$ 关于向量 $v_i\otimes w_j$ 的适当的表的矩阵是 $nm\times nm$ 矩阵 K，写作分块形式是

$$A\otimes B=\begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1m}B \\ a_{21}B & a_{22}B & \cdots & a_{2m}B \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mm}B \end{bmatrix}.$$

矩阵 $A\otimes B$ 叫做矩阵 A 和 B 的**克罗内克积**．

8.47 设 R 是整环，且 $Q=\mathrm{Frac}(R)$．如果 A 是 R-模，证明 $Q\otimes_R A$ 中的每个元素都有 $q\otimes a$ 的形式，其中 $q\in Q$ 和 $a\in A$（代替 $\sum_i q_i\otimes a_i$）．（把这个结果和例 8.89 作比较．）

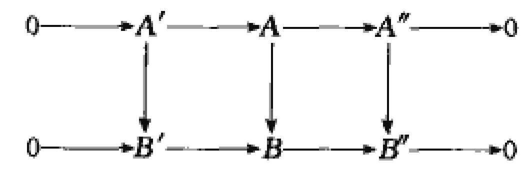
8.48 设 m 和 n 都是正整数，并设 $d=(m,n)$．证明存在阿贝尔群的同构

$$\mathbb{I}_m\otimes\mathbb{I}_n\cong\mathbb{I}_d.$$

8.49 设 k 是交换环，并设 P 和 Q 都是投射 k-模．证明 $P\otimes_k Q$ 是投射 k-模．

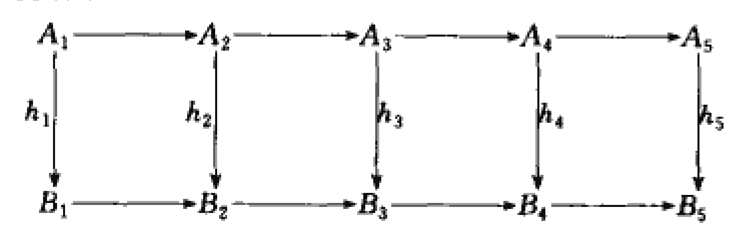
8.50 设 k 是交换环，并设 P 和 Q 都是平坦 k-模．证明 $P\otimes_k Q$ 是平坦 k-模．

8.51 假定下面的图交换，且垂直箭头都是同构.



证明底下一行是正合的当且仅当顶上一行是正合的．

8.52 （**五引理**）考虑有正合行的交换图



（ⅰ）如果 h_2 和 h_4 都是满射，h_5 是单射，证明 h_3 是满射．

604

（ⅱ）如果 h_2 和 h_4 都是单射，h_1 是满射，证明 h_3 是单射．

（ⅲ）如果 h_1，h_2，h_4 和 h_5 都是同构，证明 h_3 是同构．

8.53　证明一个环 R 是左诺特环当且仅当内射左 R-模的每个（具有有向指标集）正向极限是内射模．

提示：见定理 8.105.

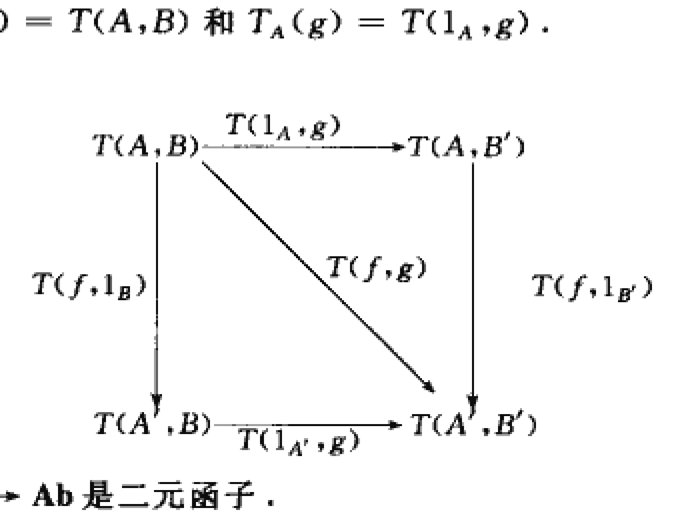
8.54　设$\mathcal{A}$，$\mathcal{B}$和$\mathcal{C}$都是范畴．一个二元函子 $T:\mathcal{A}\times\mathcal{B}\to\mathcal{C}$对对象的每个有序对 (A,B) 指定一个对象 $T(A,B)\in \text{ob}(\mathcal{C})$，其中 $A\in\text{ob}(\mathcal{A})$ 和 $B\in\text{ob}(\mathcal{B})$，并对每个态射的有序对即$\mathcal{A}$中的 $f:A\to A'$ 和$\mathcal{B}$中的 $g:B\to B'$ 指定一个态射 $T(f,g):T(A,B)\to T(A',B')$，使得

(a) 固定其中一个变量是函子：例如，如果 $A\in\text{ob}(\mathcal{A})$，则

$$T_A = T(A,\;):\mathcal{B}\to\mathcal{C}$$

是一个函子，其中 $T_A(B)=T(A,B)$ 和 $T_A(g)=T(1_A,g)$．

(b) 下图交换：



（ⅰ）证明 $\otimes$：$\mathbf{Mod}_R\times_R\mathbf{Mod}\to\mathbf{Ab}$ 是二元函子．

（ⅱ）修改二元函子的定义以允许变量中有反变，并证明 Hom 是一个二元函子．

8.5　特征标

表示论是研究抽象群 G 到非奇异矩阵群中的同态；这种同态产生数字不变量，它的算术性质可以帮助证明关于 G 的定理．我们现在以证明下述定理为目标引入这个广阔课题．

定理 8.115（伯恩赛德）　*阶为 $p^m q^n$ 的每个群 G 是可解群，其中 p 和 q 是素数．*

注意，伯恩赛德定理不能改进到阶有三个不同素因数的群，因为 A_5 是单群，阶为 $60=2^2\cdot 3\cdot 5$.

我们可以用表示证明下一定理．

605

定理　*如果 G 是非阿贝尔的有限单群，则$\{1\}$是大小为素数幂的唯一共轭类．*

命题 8.116　*上面的定理蕴涵伯恩赛德定理．*

证明　假定伯恩赛德定理不成立，并设 G 是“最小的出界者”；即 G 是阶最小的反例．如果 G 有真正规子群 H，且 $H\neq\{1\}$，则 H 和 G/H 都是可解的，这是因为它们的阶都小于 $|G|$，并有 $p^i q^j$ 的形式．根据命题 4.24，G 是可解的，这是一个矛盾．所以我们可以假定 G 是非阿贝尔单群．

设 Q 是 G 的西罗 q-子群．如果 $Q=\{1\}$，则 G 是 p-群，与 G 是非阿贝尔单群矛盾；因此 $Q\neq\{1\}$．根据定理 2.103，Q 的中心是非平凡的，我们可以选取一个非平凡元素 $x\in Z(Q)$．现在因 Q 中的每个元素和 x 可交换，所以 $Q\leqslant C_G(x)$，从而

$$[G:Q]=[G:C_G(x)][C_G(x):Q];$$

即 $[G:C_G(x)]$ 是$[G:Q]=p^m$ 的因数．当然，$[G:C_G(x)]$ 是 x 的共轭类 x^G 中元素的个数（系 2.100），从而命题假设说 $|x^G|=1$；因此 $x\in Z(G)$，与 G 是单群矛盾．■

命题的假设为真的证明要用到表示论（见定理 8.153）．

我们现在把 550 页 k-表示的定义从标量的任意域 k 局限于复数$\mathbb{C}$.

定义 群 G 的一个表示是一个同态

$$\sigma : G \to \mathrm{GL}(V),$$

其中 V 是$\mathbb{C}$上的向量空间. σ 的**次数**是 $\dim(V)$.

本节的剩下部分，我们把自己限制在有限群和次数有限的表示上. 如果一个表示 $\sigma : G \to \mathrm{GL}(V)$ 有次数 n，并选定了 V 的一组基，则每个 $\sigma(g)$ 可以看作元素在$\mathbb{C}$中的一个 $n \times n$ 非奇异矩阵.

表示可以翻译成模的语言. 在命题 8.37 中，我们证明每个表示 $\sigma: G \to \mathrm{GL}(V)$ 把 V 配置成一个左$\mathbb{C}G$-模的结构（反之亦然）：如果 $g \in G$，则 $\sigma(g) : V \to V$，对 $g \in G$ 和 $v \in V$，定义标量乘法 gv 为

$$gv = \sigma(g)(v).$$

例 8.117 我们现在证明置换表示，即 G-集[⊖]给出一个特殊类型的表示. 一个 G-集 X 对应一个同态$\pi : G \to S_X$，其中 S_X 是 X 的一切置换的对称群. 如果 V 是以 X 为基的复向量空间，则可以用下面的方式来看 $S_X \leqslant \mathrm{GL}(V)$. X 的每个置换$\pi(g)$（其中 $g \in G$）现在是 V 的基的一个置换，因此它确定 V 上的一个非奇异线性变换. 对于基 X, $\pi(g)$ 的矩阵是一个**置换矩阵**：它是把单位矩阵 I 的列换成$\pi(g)$ 形成的；于是它的每行每列恰有一个元素等于 1 而其他元素都是 0. ■

606

最重要的表示之一是正则表示；用模的术语说，正则表示是把群代数$\mathbb{C}G$看作它自身上的左模.

定义 如果 G 是群，则定义表示 $\rho : G \to \mathrm{GL}(\mathbb{C}G)$ 为对一切 $g, h \in G$，

$$\rho(g) : h \mapsto gh,$$

这个表示称为**正则表示**.

两个表示 $\sigma : G \to \mathrm{GL}(V)$ 和 $\tau : G \to \mathrm{GL}(W)$ 可以相加.

定义 如果 $\sigma: G \to \mathrm{GL}(V)$ 和 $\tau : G \to \mathrm{GL}(W)$ 都是表示，则定义它们的和 $\sigma + \tau : G \to \mathrm{GL}(V \oplus W)$ 为对一切 $g \in G, v \in V$ 和 $w \in W$，

$$(\sigma + \tau)(g) : (v, w) \mapsto (\sigma(g)v, \tau(g)w).$$

用矩阵的术语说，如果 $\sigma : G \to \mathrm{GL}(n, \mathbb{C})$ 和 $\tau : G \to \mathrm{GL}(m, \mathbb{C})$，则

$$\sigma + \tau : G \to \mathrm{GL}(n + m, \mathbb{C}),$$

并且如果 $g \in G$，则$(\sigma + \tau)(g)$是块的直和 $\sigma(g) \oplus \tau(g)$；即

$$(\sigma + \tau)(g) = \begin{bmatrix} \sigma(g) & 0 \\ 0 & \tau(g) \end{bmatrix}.$$

下面的术语在群表示中是普遍使用的.

定义 群 G 的一个表示是**不可约的**，如果对应的$\mathbb{C}G$-模是单的；一个表示 σ 是**完全可约的**，如果它是不可约表示的直和；即对应的$\mathbb{C}G$-模是半单的.

例 8.118 一个表示 σ 是**线性**的，如果 $\mathrm{degree}(\sigma) = 1$. 因为主模 $V_0(\mathbb{C})$是一维的，所以任意群 G 的平凡表示都是线性的. 如果 $G = S_n$，则 $\mathrm{sgn} : G \to \{\pm 1\}$ 也是线性表示.

每个线性表示是不可约的，这是因为对应的$\mathbb{C}G$-模必是单的；毕竟每个子模都是子空间，而一维向量空间 V 只有子空间 $\{0\}$ 和 V. 由此，任意群 G 的平凡表示和 S_n 的表示 sgn 一样是不可约的. ■

607

回忆韦德伯恩-阿廷定理的证明：在$\mathbb{C}G$ 中存在两两不同构的极小左理想 $L_1, \cdots, L_r$ 和$\mathbb{C}G =$

⊖ 回忆如果群 G 作用在集合 X 上，则 X 叫做 G-集.

$B_1 \oplus \cdots \oplus B_r$，其中 B_i 由一切同构于 L_i 的极小左理想生成．现在根据系 8.65，$B_i \cong \mathrm{Mat}_{n_i}(\mathbb{C})$．但根据引理 8.61（ⅱ），$\mathrm{Mat}_{n_i}(\mathbb{C})$ 中的一切极小左理想都同构，因此 $L_i \cong \mathrm{COL}(1) \cong \mathbb{C}^{n_i}$（见例 8.30）．所以

$$B_i \cong \mathrm{End}(L_i),$$

这里我们已经把 $\mathrm{End}_{\mathbb{C}}(L_i)$ 缩写为 $\mathrm{End}(L_i)$.

命题 8.119 （ⅰ）对$\mathbb{C}G$中的每个极小左理想 L_i，存在不可约表示 $\lambda_i : G \to \mathrm{GL}(L_i)$，它由左乘映射

$$\lambda_i(g) : u_i \mapsto gu_i$$

给出，其中 $g \in G$ 和 $u_i \in L_i$；此外，$\mathrm{degree}(\lambda_i) = n_i = \dim(L_i)$.

（ⅱ）如果对 $g \in G$ 和 $u_j \in B_j$，定义

$$\widetilde{\lambda}_i(g)u_j = \begin{cases} gu_i & \text{如果 } j = i \\ 0 & \text{如果 } j \neq i \end{cases} \tag{2}$$

则表示 λ_i 扩张为$\mathbb{C}$-代数映射 $\widetilde{\lambda}_i : \mathbb{C}G \to \mathbb{C}G$.

证明 （ⅰ）因 L_i 是$\mathbb{C}G$中的左理想，每个 $g \in G$ 由左乘作用在 L_i 上，因此 G 的对应的表示 λ_i 如所陈述的那样；因为极小左理想是单模，所以它是一个不可约表示．

（ⅱ）如果把$\mathbb{C}G$和 $\mathrm{End}(L_i)$看作$\mathbb{C}$上的向量空间，则 λ_i 扩张为线性变换 $\widetilde{\lambda}_i : \mathbb{C}G \to \mathrm{End}(L_i)$（因为 G 的元素是$\mathbb{C}G$的基）：

$$\widetilde{\lambda}_i : \sum_g c_g g \mapsto \sum_g c_g \lambda_i(g).$$

我们证明 $\widetilde{\lambda}_i : \mathbb{C}G \to \mathrm{End}(L_i)$ 确实是一个$\mathbb{C}$-代数映射．如果 $u_i \in L_i$ 和 g，$h \in G$，则

$$\widetilde{\lambda}_i(gh) : u_i \mapsto (gh)u_i,$$

而

$$\widetilde{\lambda}_i(g)\widetilde{\lambda}_i(h) : u_i \mapsto hu_i \mapsto g(hu_i);$$

由结合性，它们相等．

代数$\mathbb{C}G = B_1 \oplus \cdots \oplus B_r$，其中每个 B_i 不仅是 R 中的双边理想，而且它“几乎”是 R 的子环（它的幺元和$\mathbb{C}G$中的幺元不同）。定义$\mathbb{C}$-线性变换 $F : \mathbb{C}G \to \mathbb{C}G$ 为

$$F : (b_1, \cdots, b_r) \mapsto (\widetilde{\lambda}_1(b_1), \cdots, \widetilde{\lambda}_r(b_r)).$$

为证明 F 是$\mathbb{C}$-代数映射，只要证明它保持乘法．已经证明只要 b_i，$b_i' \in B_i$ 就有

$$F(b_ib_i') = \widetilde{\lambda}_i(b_ib_i') = \widetilde{\lambda}_i(b_i)\widetilde{\lambda}_i(b_i') = F(b_i)F(b_i').$$

但如果 $b_i \in B_i$ 和 $b_j \in B_j$，其中 $i \neq j$，则 $b_ib_j = 0$（因为每个 B 都是理想且$\mathbb{C}G$是它们的直和）．另一方面，$F(b_i) \in B_i$ 和 $F(b_j) \in B_j$，从而 $F(b_i)F(b_j) = 0$．即 $F(b_ib_j) = 0 = F(b_i)F(b_j)$，所以 F 是代数映射． ■

608

如果两个表示所对应的模同构，则自然称这两个表示等价．

定义 假定 G 是群，σ，$\tau : G \to \mathrm{GL}(n, \mathbb{C})$ 都是表示，则称 σ 和 τ **等价**，记为 $\sigma \sim \tau$，如果存在非奇异 $n \times n$ 矩阵 P 交结它们；即对每个 $g \in G$，

$$P\sigma(g)P^{-1} = \tau(g).$$

当然，这个定义来自系 8.39，它说$\mathbb{C}G$-模 $(\mathbb{C}^n)^\sigma$ 和 $(\mathbb{C}^n)^\tau$ 作为$\mathbb{C}G$-模同构当且仅当$\sigma \sim \tau$.

系 8.120 （ⅰ）有限群 G 的每个不可约表示等价于命题 8.119（ⅰ）给出的表示 λ_i 之一．

（ⅱ）有限阿贝尔群的每个不可约表示都是线性的．

（ⅲ）如果 $\sigma: G \to \mathrm{GL}(V)$ 是有限群 G 的表示，则对每个 $g \in G$，$\sigma(g)$ 与一个对角矩阵相似．

证明　（ⅰ）如果 $\sigma: G \to \mathrm{GL}(V)$ 是一个不可约表示 σ，则对应的 $\mathbb{C}G$-模 V^σ 是单模．所以根据命题 8.54，有某个 i 使得 $V^\sigma \cong L_i$．但 $L_i \cong V^{\lambda_i}$，因此 $V^\sigma \cong V^{\lambda_i}$ 和 $\sigma \sim \lambda_i$．

（ⅱ）因 G 是阿贝尔群，$\mathbb{C}G = \sum_i B_i$ 是交换的，因此一切 $n_i = 1$．但 $n_i = \mathrm{degree}(\lambda_i)$．

（ⅲ）如果 $\sigma' = \sigma \mid \langle g \rangle$，则 $\sigma'(g) = \sigma(g)$．现在 σ' 是阿贝尔群 $\langle g \rangle$ 的表示，因此（ⅱ）蕴涵模 $V^{(\sigma')}$ 是一维子模的直和．如果 $V^{(\sigma')} = \langle v_1 \rangle \oplus \cdots \oplus \langle v_m \rangle$，则 $\sigma(g)$ 关于基 $v_1, \cdots, v_m$ 的矩阵是对角矩阵．■

例 8.121　（ⅰ）可以这样重述韦德伯恩-阿廷定理，每个表示 $\tau: G \to \mathrm{GL}(V)$ 都是完全可约的：$\tau = \sigma_1 + \cdots + \sigma_k$，其中每个 σ_j 都是不可约的；此外，每个 σ_j 的重数由 τ 唯一确定．因每个 σ_j 等价于某个 λ_i，我们常合并项而写作 $\tau \sim \sum_i m_i \lambda_i$，其中重数 m_i 是非负整数．

（ⅱ）正则表示 $\rho: G \to \mathbb{C}G$ 的重要性在于每个不可约表示都是它的直和项．现在 ρ 等价于和

$$\rho \sim n_1\lambda_1 + \cdots + n_r\lambda_r,$$

其中 n_i 是 λ_i 的次数［回忆 $\mathbb{C}G = \sum_i B_i$，其中 $B_i \cong \mathrm{End}(L_i) \cong \mathrm{Mat}_{n_i}(\mathbb{C})$，单模 L_i 作为 $\mathbb{C}G$-模可以看作 $n_i \times n_i$ 矩阵的第一列，从而 B_i 是 L_i 的 n_i 个复制的直和］．■　609

回忆元素在交换环 k 中的 $n \times n$ 矩阵 $A = [a_{ij}]$ 的**迹**是对角线元素的和：$\mathrm{tr}(A) = \sum_{i=1}^{n} a_{ii}$．

当 k 是域时，$\mathrm{tr}(A)$ 是 A 的特征值的和（现在要假定有这个结果，但更适当的是在下一章中证明它）．下面是关于迹的另外两个基本事实，我们现在给出证明．

命题 8.122　（ⅰ）如果 $A = [a_{ij}]$ 和 $B = [b_{ij}]$ 是元素在交换环 k 中的 $n \times n$ 矩阵，则

$$\mathrm{tr}(A+B) = \mathrm{tr}(A) + \mathrm{tr}(B) \text{ 和 } \mathrm{tr}(AB) = \mathrm{tr}(BA).$$

（ⅱ）如果 $B = PAP^{-1}$，则 $\mathrm{tr}(B) = \mathrm{tr}(A)$．

证明　（ⅰ）迹的加性由 $A+B$ 的对角线元素为 $a_{ii} + b_{ii}$ 可得．如果用 $(AB)_{ii}$ 表示 AB 的 ii 元素，则

$$(AB)_{ii} = \sum_j a_{ij} b_{ji},$$

因此

$$\mathrm{tr}(AB) = \sum_i (AB)_{ii} = \sum_{i,j} a_{ij} b_{ji}.$$

同样，

$$\mathrm{tr}(BA) = \sum_{j,i} b_{ji} a_{ij}.$$

因为元素都在交换环 k 中，所以它们可交换，从而对一切 i, j，$a_{ij} b_{ji} = b_{ji} a_{ij}$．由此得到所要的 $\mathrm{tr}(AB) = \mathrm{tr}(BA)$．

（ⅱ）

$$\mathrm{tr}(B) = \mathrm{tr}((PA)P^{-1}) = \mathrm{tr}(P^{-1}(PA)) = \mathrm{tr}(A).$$ ■

由（ⅱ），我们可以定义线性变换 $T: V \to V$ 的迹为由它产生的任一矩阵的迹，其中 V 是域 k 上的向量空间：如果 A 和 B 都是 T 的矩阵，它们由 V 的两组基确定，则有某个非奇异矩阵 P 使得 $B = PAP^{-1}$，因此 $\mathrm{tr}(B) = \mathrm{tr}(A)$．

定义　如果 $\sigma: G \to \mathrm{GL}(V)$ 是表示，则它的**特征标**是指由

$$\chi_\sigma(g) = \mathrm{tr}(\sigma(g))$$

定义的函数 $\chi_\sigma : G \to \mathbb{C}$；我们称 χ_σ 为 σ **提供的特征标**．**不可约特征标**是指一个不可约表示提供的特征标．定义 χ_σ 的**次数**为 σ 的次数；即

610

$$\mathrm{degree}(\chi_\sigma) = \mathrm{degree}(\sigma) = \dim(V).$$

例 8.123 （ⅰ）由线性表示（见例 8.118）提供的特征标 θ 叫做**线性特征标**；即 $\theta=\chi_\sigma$，其中 $\mathrm{degree}(\sigma)=1$. 因每个线性表示都是单的，所以每个线性特征标都是不可约的．

（ⅱ）表示 $\lambda_i : G \to \mathrm{GL}(L_i)$［见命题8.119(ⅰ)］是不可约的．于是由 λ_i 提供的特征标

$$\chi_i = \chi\lambda_i$$

是不可约的．

（ⅲ）根据命题8.119(ⅱ)，对每个 $u \in \mathbb{C}G$ 说 $\chi_i(u)$ 是有意义的．当然，当 $j\neq i$ 时，对一切 $u_j \in \mathrm{End}(L_j)$ 有 $\chi_i(u_j) = 0$，从而

$$\chi_i(u_j) = \begin{cases} \mathrm{tr}(\widetilde{\lambda}_i(u_j)) & \text{如果 } j = i \\ 0 & \text{如果 } j \neq i. \end{cases}$$

（ⅳ）如果 $\sigma : G \to \mathrm{GL}(V)$ 是任一表示，则 $\chi_\sigma(1) = n$，其中 n 是 σ 的次数．毕竟 $\sigma(1)$ 是单位矩阵，它的迹是 $n = \dim(V)$．

（ⅴ）设 $\sigma : G \to S_X$ 是同态；和例 8.117 一样，可以把 σ 看作 V 上的表示，其中 V 是$\mathbb{C}$上以 X 为基的向量空间．对每个 $g \in G$，矩阵 $\sigma(g)$ 是置换矩阵，如果 $\sigma(g)x = x$，则它的第 x 个对角线元素为 1，否则为 0. 于是

$$\chi_\sigma(g) = \mathrm{tr}(\sigma(g)) = \mathrm{Fix}(\sigma(g)),$$

$\mathrm{Fix}(\sigma(g))$ 是被 $\sigma(g)$ 固定的 $x \in X$ 的个数．换句话说，如果 X 是一个 G-集，则可以把每个 $g\in G$ 看作作用在 X 上，g 的作用的**固定点**的个数就是特征标值（相关讨论见例 8.144）． ■

特征标和表示的加法相容：如果 $\sigma : G \to \mathrm{GL}(V)$ 和 $\tau : G \to \mathrm{GL}(W)$，则 $\sigma+\tau : G \to \mathrm{GL}(V\oplus W)$，且

$$\mathrm{tr}((\sigma+\tau)(g)) = \mathrm{tr}\left(\begin{bmatrix} \sigma(g) & 0 \\ 0 & \tau(g) \end{bmatrix}\right) = \mathrm{tr}(\sigma(g)) + \mathrm{tr}(\tau(g)).$$

所以，

$$\chi_{\sigma+\tau} = \chi_\sigma + \chi_\tau.$$

如果 σ 和 τ 是等价表示，则对一切 $g \in G$，

$$\mathrm{tr}(\sigma(g)) = \mathrm{tr}(P\sigma(g)P^{-1}) = \mathrm{tr}(\tau(g)).$$

即它们有相同的特征标：$\chi_\sigma = \chi_\tau$．由此，如果 $\sigma : G \to \mathrm{GL}(V)$ 是表示，则它的特征标 χ_σ 可以用 V 的任意一个合适的基来计算．

611

命题 8.124 （ⅰ）*每个特征标 χ_σ 都是由 $\lambda_i : G \to \mathrm{GL}(L_i)$ 提供的不可约特征标 $\chi_i=\chi_{\lambda_i}$ 的 $\mathbb{N}$-线性组合：存在整数 $m_i\geqslant 0$ 使得*

$$\chi_\sigma = \sum_i m_i \chi_i.$$

（ⅱ）*等价表示有相同的特征标．*

（ⅲ）*G 的不可约特征标只有 $\chi_1,\cdots,\chi_r$.*

证明 （ⅰ）特征标 χ_σ 由 G 的表示 σ 产生，而表示 σ 由$\mathbb{C}G$-模 V 产生．但 V 是半单模（因为 $\mathbb{C}G$ 是半单环），从而 V 是单模的直和：$V=\sum_j S_j$．根据命题8.54，有某个极小左理想 L_i 使得每个 $S_j\cong L_i$．如果对每个 i，令 $m_i\geqslant 0$ 是同构于 L_i 的 S_j 的个数，则 $\chi_\sigma=\sum_i m_i\chi_i$．

（ⅱ）由命题8.122的（ⅱ）和系8.120(ⅰ)得到．

（ⅲ）由（ⅱ）和系8.120(ⅰ)得到． ■

作为这个命题的一个推论，我们称 $\chi_1,\cdots,\chi_r$ 为 G 的**不可约特征标**．

例 8.125 （ⅰ）对一切 $g\in G$，具有 $\sigma(g)=1$ 的平凡表示 $\sigma:G\to\mathbb{C}$所提供的（线性）特征标 χ 叫做**平凡特征标**．于是对一切 $g\in G$，$\chi_1(g)=1$.

（ⅱ）我们计算由正则表示 $\rho:G\to\mathrm{GL}(\mathbb{C}G)$ 提供的**正则特征标**$\psi=\chi_\rho$，其中对一切 $g\in G$ 和 $u\in\mathbb{C}G$，$\rho(g):u\mapsto gu$．$\mathbb{C}G$ 的任意一个基都可以用于这个计算；我们选取由 G 的元素组成的通常的基．如果 $g=1$，则例8.123（ⅳ）表明 $\psi(1)=\dim(\mathbb{C}G)=|G|$．另一方面，如果 $g\neq 1$，则对一切 $h\in G$，gh 是与 h 不同的一个基元素．所以 $\rho(g)$的矩阵的对角线上的元素为 0，从而它的迹是 0. 于是，

$$\psi(g)=\begin{cases}0 & \text{如果 } g\neq 1\\ |G| & \text{如果 } g=1.\end{cases}$$ ■

我们已经证明了等价表示有相同的特征标．接下来的讨论将给出逆命题：如果两个表示有相同的特征标，则它们等价．

定义 一个函数 $\varphi:G\to\mathbb{C}$ 称为**类函数**，如果它在共轭类上是常数；即如果 $h=xgx^{-1}$，则 $\varphi(h)=\varphi(g)$．

612

由表示 σ 提供的每个特征标 χ_σ 是一个类函数：如果 $h=xgx^{-1}$，则

$$\sigma(h)=\sigma(xgx^{-1})=\sigma(x)\sigma(g)\sigma(x)^{-1},$$

从而 $\mathrm{tr}(\sigma(h))=\mathrm{tr}(\sigma(g))$；即

$$\chi_\sigma(h)=\chi_\sigma(g).$$

不是每个类函数都是特征标．例如，如果 χ 是特征标，则 $-\chi$ 是一个类函数；因为 $-\chi(1)$是负的，所以它不是特征标，从而它不可能有次数．

定义 记一切类函数的集合 $G\to\mathbb{C}$ 为 $\mathrm{cf}(G)$：

$$\mathrm{cf}(G)=\{\varphi:G\to\mathbb{C}:\text{对一切 } x,g\in G,\varphi(g)=\varphi(xgx^{-1})\}.$$

易知 $\mathrm{cf}(G)$是$\mathbb{C}$上的向量空间．

一个元素 $u=\sum_{g\in G}c_g g\in\mathbb{C}G$是复数的$n$ 元组 (c_g)；即 u 是一个函数$u:G\to\mathbb{C}$，对一切 $g\in G$有 $u(g)=c_g$．由此，我们知道 $\mathrm{cf}(G)$是$\mathbb{C}G$ 的子环．注意每一个类和都是一个类函数；所以引理 8.68 说 $\mathrm{cf}(G)$是中心 $Z(\mathbb{C}G)$，从而

$$\dim(\mathrm{cf}(G))=r,$$

其中 r 是G 中共轭类的个数（见定理8.69）．

定义 记$\mathbb{C}G=B_1\oplus\cdots\oplus B_r$，其中 $B_i\cong\mathrm{End}(L_i)$，并令 e_i 表示 B_i 的幺元；因此

$$1=e_1+\cdots e_r,$$

其中 1 是$\mathbb{C}G$的幺元．元素 e_i 称为$\mathbb{C}G$中的幂等元．

每个 e_i 不只是幂等元，即 $e_i^2=e_i$，而且易知

$$e_ie_j = \delta_{ij}e_i,$$

其中 δ_{ij} 是克罗内克 δ.

引理 8.126 不可约特征标 χ_1，…，χ_r 形成 $\mathrm{cf}(G)$的基．

证明 我们已经看到 $\dim(\mathrm{cf}(G)) = r$，从而根据系 3.89（ⅱ），只需证明 χ_1，…，χ_r 是线性无关表．我们已经注意到对一切 $j\neq i$，$\chi_i(u_j)=0$；特别地，$\chi_i(e_j)=0$．另一方面，$\chi_i(e_i)=n_i$，其中 n_i 是 χ_i 的次数，这是因为 n_i 是 $n_i\times n_i$ 单位矩阵的迹．

现在假设 $\sum\limits_i c_i\chi_i=0$．由此对一切 j 有

$$0=\Big(\sum_i c_i\chi_i\Big)(e_j)=c_j\chi_j(e_j)=c_jn_j.$$

[613] 所以正如所要的，一切 $c_j=0$. ■

定理 8.127 有限群 G 的两个表示等价当且仅当它们提供相同的特征标：$\chi_\sigma=\chi_\tau$．

证明 在命题8.124(ⅱ)中已经证明了必要性．关于充分性，命题8.124(ⅱ)说每个表示都是完全可约的：存在非负整数 m_i 和ℓ_i使得 $\sigma\sim\sum\limits_i m_i\lambda_i$ 和 $\tau\sim\sum\limits_i\ell_i\lambda_i$．根据假设，对应的特征标一致：

$$\sum_i m_i\chi_i=\chi_\sigma=\chi_\tau=\sum_i\ell_i\chi_i.$$

因为不可约特征标 χ_1，…，χ_r 是 $\mathrm{cf}(G)$的基，所以对一切 i，$m_i=\ell_i$，因此 $\sigma\sim\tau$. ■

不可约特征标之间存在一种关系，使得对它们的计算变得容易．我们先求幂等元 e_i 在$\mathbb{C}G$的基 G 下的表达式．根据例8.123(ⅳ)，$\chi_i(1)=n_i$，它是 λ_i 的次数．另一方面，根据命题 8.119 中的等式（2），如果 $j\neq i$，有 $\chi_i(e_j)=0$，从而

$$n_i=\chi_i(1)=\sum_j\chi_i(e_j)=\chi_i(e_i)^{\ominus}. \tag{3}$$

我们还看到对一切 $y\in G$，因为 $y=\sum\limits_j e_jy$ 和 $e_jy\in B_j$，所以有 $\chi_i(y)=\sum\limits_j\chi_i(e_jy)=\chi_i(e_iy)$，从而

$$\chi_i(e_iy)=\chi_i(y), \tag{4}$$

命题 8.128 如果 $e_i=\sum\limits_{g\in G}a_{ig}g$，其中 $a_{ig}\in\mathbb{C}$，则

$$a_{ig}=\frac{n_i\chi_i(g^{-1})}{|G|}.$$

证明 设ψ是正则特征标；即ψ是正则表示提供的特征标．现在 $e_ig^{-1}=\sum\limits_h a_{ih}hg^{-1}$，从而

$$\psi(e_ig^{-1})=\sum_{h\in G}a_{ih}\psi(hg^{-1}).$$

根据例8.125(ⅱ)，当 $h=g$ 时 $\psi(1)=|G|$，当 $h\neq g$ 时$\psi(hg^{-1})=0$．所以

⊖ 式（3）的证明是正确的，但我们在引理 8.126 中已经用另一种方法证明了它，在那里是注意到 $\chi_i(1)$ 是 $n_i\times n_i$ 单位矩阵的迹而证明的.

$$a_{ig} = \frac{\psi(e_i g^{-1})}{|G|}.$$

另一方面，因 $\psi = \sum_j n_j \chi_j$，根据命题 8.119 等式 (2) 有

$$\psi(e_i g^{-1}) = \sum_j n_j \chi_j(e_i g^{-1}) = n_i \chi_i(e_i g^{-1}),$$

但根据等式 (4)，$\chi_i(e_i g^{-1}) = \chi_i(g^{-1})$. 所以，$a_{ig} = n_i \chi_i(g^{-1}) / |G|$. ■

现在可以方便地给 cf(G)配置一个内积. [614]

定义 如果 α，$\beta \in \mathrm{cf}(G)$，定义

$$(\alpha,\beta) = \frac{1}{|G|}\sum_{g\in G}\alpha(g)\overline{\beta(g)},$$

其中 $\bar{c}$ 表示复数 c 的复共轭.

易知我们定义了一个内积；⊖ 即对一切 c_1，$c_2 \in \mathbb{C}$，

(i) $(c_1\alpha_1 + c_2\alpha_2, \beta) = c_1(\alpha_1,\beta) + c_2(\alpha_2,\beta)$；

(ii) $(\beta,\alpha) = \overline{(\alpha,\beta)}$.

注意，根据 (ii)，(α,α)是实数且内积是确定的；即如果 $\alpha \neq 0$，则$(\alpha,\alpha) > 0$.

定理 8.129 关于刚才定义的内积，不可约特征标 $\chi_1,\cdots,\chi_r$ 形成一个正交基；即

$$(\chi_i,\chi_j) = \delta_{ij}.$$

证明 根据命题 8.128，有

$$e_j = \frac{1}{|G|}\sum_g n_j \chi_j(g^{-1})g.$$

因此，

$$\begin{aligned}\chi_i(e_j)/n_j &= \frac{1}{|G|}\sum_g \chi_j(g^{-1})\chi_i(g) \\ &= \frac{1}{|G|}\sum_g \chi_i(g)\overline{\chi_j(g)} \\ &= (\chi_i,\chi_j);\end{aligned}$$

上面等式中的倒数第二个等式从习题 8.56 (ii) 得来，因为 χ_j 是特征标（不仅仅是类函数），从而 $\chi_j(g^{-1}) = \overline{\chi_j(g)}$. 现在根据等式 (2) 和 (3)，$\chi_i(e_j)/n_j = \delta_{ij}$，结果由此可得. ■

cf(G) 上的内积可以用来验证不可约性.

定义 有限群 G 上的**广义特征标** φ 是线性组合

$$\varphi = \sum_i m_i \chi_i,$$

其中 χ_1，…，χ_r 是 G 的不可约特征标，系数 $m_i \in \mathbb{Z}$.

如果 θ 是一个特征标，则根据命题 8.124，$\theta = \sum_i m_i \chi_i$，其中一切系数都是非负整数. [615]

系 8.130 群 G 的一个广义特征标 θ 是不可约特征标当且仅当 $\theta(1) > 0$ 且

⊖ 这个内积不是双线性型，因为有 $(\beta,\alpha) = \overline{(\alpha,\beta)}$，而不是 $(\beta,\alpha) = (\alpha,\beta)$. 这种函数常叫做埃尔米特型或半双线性型 (sesquilinear form，sesqui 的意思是"一个半").

$$(\theta,\theta) = 1.$$

证明 如果 θ 是不可约特征标，则有某个 i 使得 $\theta=\chi_i$，从而 $(\theta,\theta) = (\chi_i,\chi_i) = 1$．此外，$\theta(1) = \deg(\chi_i) > 0$．

反之，设 $\theta = \sum_i m_j \chi_j$，其中 $m_j \in \mathbb{Z}$，并假设 $(\theta,\theta) = 1$，则 $1 = \sum_j m_j^2$．因此某个 $m_i^2 = 1$ 而其他 $m_j = 0$．所以，$\theta = \pm \chi_i$，从而 $\theta(1) = \pm \chi_i(1)$．因 $\chi_i(1) = \deg(\chi_i) > 0$，命题的假设 $\theta(1) > 0$ 给出 $m_i = 1$．所以，$\theta = \chi_i$，因此 θ 是不可约特征标． ■

我们配备从现在起要使用的记号．

记号 如果 G 是有限群，记它的共轭类为

$$C_1,\cdots,C_r,$$

从每个共轭类选取一个元素记为

$$g_1 \in C_1,\cdots,g_r \in C_r,$$

它的不可约特征标记为

$$\chi_1,\cdots,\chi_r,$$

它们的次数记为

$$n_1 = \chi_1(1),\cdots,n_r = \chi_r(1),$$

共轭类的大小记为

$$h_1 = |C_1|,\cdots,h_r = |C_r|.$$

矩阵 $[\chi_i(g_j)]$ 是表达信息的有用方法．

定义 G 的**特征标表**是指 ij 元素为 $\chi_i(g_j)$ 的 $r \times r$ 复数矩阵．

我们恒假定 $C_1 = \{1\}$ 和 χ_1 是平凡特征标．于是，第一行都是 1，而第一列由特征标的次数组成：根据例8.123(ⅳ)，对一切 i，$\chi_i(1) = n_i$．特征标表的第 i 行由值

$$\chi_i(1),\chi_i(g_2),\cdots,\chi_i(g_r)$$

组成．没有显而易见的方法可以用来给其他的共轭类加标（或其他的不可约特征标），所以一个有限群 G 有许多特征标表．然而，我们还是常说 G 的特征标表．

因 $\mathrm{cf}(G)$ 上的内积是对一切 $g \in G$ 取和的，而不只是对选取的 g_i（一个共轭类取一个）求和，可以用“加权”内积改写它：

$$(\chi_i,\chi_j) = \frac{1}{|G|}\sum_{k=1}^{r} h_k \chi_i(g_k)\overline{\chi_j(g_k)}.$$

616 定理 8.129 说特征标表中不同行的加权内积是 0，而任一行和它自己的加权内积是 1.

例 8.131 特征标表的元素可以是复数．例如，易知 3 阶循环群 $G=\langle x\rangle$ 的特征标表由表 8.1 给出，其中 $\omega = e^{2\pi i/3}$ 是三次单位原根． ■

例 8.132 用加法记号写出四群：

$$\mathbf{V} = \{0,a,b,a+b\}.$$

作为 $\mathbb{F}_2$ 上的向量空间，$\mathbf{V}$ 有基 a,b，取值于$\{1,-1\}\subseteq\mathbb{C}$ 的 $\mathbf{V}$ 上的“坐标函数”是线性的，因而是不可约表示．例如，在 a 上非平凡而在 b 上平凡的函数形成的特征标 χ_2 是

$$\chi_2(v)=\begin{cases}-1 & 如果\ v=a\ 或\ v=a+b\\ 1 & 如果\ v=0\ 或\ v=b.\end{cases}$$

表 8.2 是特征标表. ■

表 8.1　$\mathbb{I}_3$ 的特征标表

g_i	1	x	x^2
h_i	1	1	1
χ_1	1	1	1
χ_2	1	ω	ω^2
χ_3	1	ω^2	ω

表 8.2　V 的特征标表

g_i	0	a	b	$a+b$
h_i	1	1	1	1
χ_1	1	1	1	1
χ_2	1	-1	1	-1
χ_3	1	1	-1	-1
χ_4	1	-1	-1	1

例 8.133　表 8.3 是对称群 $G=S_3$ 的特征标表. 因 S_n 中的两个置换共轭当且仅当它们有相同的轮换结构，所以有三个共轭类，从每个共轭类中选取元素 1,(1 2) 和(1 2 3). 在例8.71(ⅰ)中，我们知道有三个不可约表示：λ_1＝平凡表示，$\lambda_2=\mathrm{sgn}$，第三个表示 λ_3 的次数为 2. 我们现在给出特征标表，然后讨论它的元素.

表 8.3　S_3 的特征标表

g_i	1	(1 2)	(1 2 3)
h_i	1	3	2
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

我们已经讨论过任意特征标表的第一行和第一列. 因 $\chi_2=\mathrm{sgn}$，第二行记录了 1 和 (1 2 3) 是偶置换而 (1 2) 是奇置换的事实. 第三行的元素为

$$2\quad a\quad b,$$

其中 a 和 b 待求. 第三行和其他两行的加权内积给出方程

$$2+3a+2b=0$$
$$2-3a+2b=0.$$

容易推出 $a=0$ 和 $b=-1$. ■

下面的引理将用来描述特征标表的列的内积.

引理 8.134　*如果 A 是有限群 G 的特征标表，则 A 是非奇异的，它的逆 A^{-1} 的 ij 元素为*

$$(A^{-1})_{ij}=\frac{h_i\overline{\chi_j(g_i)}}{|G|}.$$

证明　如果 B 是 ij 元素如陈述所示的矩阵，则因 $h_k\overline{\chi_j(g_k)}=\sum_{y\in C_k}\overline{\chi_j(y)}$，有

$$\begin{aligned}(AB)_{ij}&=\frac{1}{|G|}\sum_k\chi_i(g_k)h_k\overline{\chi_j(g_k)}\\&=\frac{1}{|G|}\sum_g\chi_i(g)\overline{\chi_j(g)}\\&=(\chi_i,\chi_j)\\&=\delta_{ij},\end{aligned}$$

所以 $AB=I$. ■

下一结果是基本的.

617～618

定理 8.135 (正交关系)　*设 G 是 n 阶有限群，它的共轭类为 $C_1,\cdots,C_r$，它们的基数分别为 $h_1,\cdots,h_r$，并选取元素 $g_i\in C_i$. 设 G 的不可约特征标为 $\chi_1,\cdots,\chi_r$，并设 χ_i 的次数为 n_i. 则下面*

的关系成立：

（ⅰ）

$$\sum_{k=1}^{r} h_k \chi_i(g_k) \overline{\chi_j(g_k)} = \begin{cases} 0 & \text{当 } i \neq j; \\ |G| & \text{当 } i = j. \end{cases}$$

（ⅱ）

$$\sum_{i=1}^{r} \chi_i(g_k) \overline{\chi_j(g_\ell)} = \begin{cases} 0 & \text{当 } k \neq \ell; \\ |G|/h_k & \text{当 } k = \ell. \end{cases}$$

证明 （ⅰ）这是定理 8.129 的复述．

（ⅱ）如果 A 是 G 的特征标表和 $B = [h_i \overline{\chi_j(g_i)} / |G|]$．在引理 8.134 中，我们证明了 $AB = I$．由此，$BA = I$；即 $(BA)_{k\ell} = \delta_{k\ell}$．所以

$$\frac{1}{|G|} \sum_i h_k \overline{\chi_i(g_k)} \chi_i(g_\ell) = \delta_{k\ell},$$

这就是第二个正交关系．■

对于特征标表，第二个正交关系说不同列的通常内积（不加权，但有复共轭）是 0，而对每个 k，k 列和它自己的通常内积是 $|G|/h_k$.

正交关系产生下面的特殊情形．

系 8.136 （ⅰ） $|G| = \sum_{i=1}^{r} n_i^2$.

（ⅱ）如果 $k > 1$，$\sum_{i=1}^{r} n_i \chi_i(g_k) = 0$.

（ⅲ）如果 $i > 1$，$\sum_{k=1}^{r} h_k \chi_i(g_k) = 0$.

（ⅳ）$\sum_{k=1}^{r} h_k |\chi_i(g_k)|^2 = |G|$.

证明 （ⅰ）这个等式记录了第一列和它自己的内积：它是定理8.135（ⅱ）当 $k = \ell = 1$ 时的情形.

（ⅱ）这是定理8.135（ⅱ）当 $\ell = 1$，$\chi_i(1) = n_i$ 时的特殊情形．

（ⅲ）这是定理8.135（ⅰ）当 $j = 1$ 时的特殊情形．

（ⅳ）这是定理8.135（ⅰ）当 $j = i$ 时的特殊情形．■

我们现在可以给出定理 2.113，即伯恩赛德引理的另一个证明，该定理计算了一个 G-集的轨道个数．

619

定理 8.137（伯恩赛德引理） 设 G 是有限群，并设 X 是有限 G-集．如果 N 是 X 的轨道个数，则

$$N = \frac{1}{|G|} \sum_{g \in G} \text{Fix}(g),$$

其中 $\text{Fix}(g)$ 是满足 $gx = x$ 的 $x \in X$ 的个数．

证明 设 V 是以 X 为基的复向量空间．和例 8.117 一样，G-集 X 给出对一切 $g \in G$ 和 $x \in X$ 有 $\sigma(g)(x) = gx$ 的表示 $\sigma: G \to \text{GL}(V)$；此外，如果 χ_σ 是 σ 提供的特征标，则例8.123（ⅴ）证明

$\chi_\sigma(g) = \mathrm{Fix}(g)$.

设 $O_1, \cdots, O_N$ 是 X 的轨道．我们先证明 $N=\dim(V^G)$，其中 V^G 是固定点的空间：

$$V^G=\{v\in V : 对一切\ g\in G\ 有\ gv=v\}.$$

对每个 i，定义 s_i 为 O_i 中一切 x 的和；只要证明这些元素形成 V^G 的基．显然 $s_1, \cdots, s_N$ 是 V^G 中的线性无关表，剩下要证明它们张成 V^G. 如果 $u\in V^G$，则 $u = \sum_{x\in X} c_x x$，从而 $gu = \sum_{x\in X} c_x (gx)$. 然而因 $gu=u$，所以 $c_x = c_{gx}$．于是，给定 $x\in X$ 且 $x\in O_j$，对 $g\in G$，gx 的每个系数等于 c_x；即在轨道 O_j 中的一切 x 都有相同的系数，比如 c_j，因此 $u = \sum_j c_j s_j$．所以，

$$N = \dim(V^G).$$

现在定义一个线性变换 $T: V\to V$ 为

$$T = \frac{1}{|G|}\sum_{g\in G}\sigma(g).$$

不难验证 T 是 $\mathbb{C}G$-映射，$T\mid(V^G)$ = 恒等映射，$\mathrm{im}T=V^G$. 因 $\mathbb{C}G$ 是半单的，有某个子模 W 使得 $V=V^G\oplus W$．我们断言 $T\mid W=0$. 如果 $w\in W$，则因 W 是子模，$\sigma(g)(w)\in W$，从而 $T(w)\in W$. 另一方面，$T(w)\in \mathrm{im}T = V^G$，因此正如所要的 $T(w)\in V^G\cap W=\{0\}$．

如果 $w_1, \cdots, w_\ell$ 是 W 的基，则 $s_1, \cdots, s_N, w_1, \cdots, w_\ell$ 是 $V=V^G\oplus W$ 的基．注意 T 固定每个 s_i 而零化每个 w_j. 因迹保持和，

$$\begin{aligned}\mathrm{tr}(T) &= \frac{1}{|G|}\sum_{g\in G}\mathrm{tr}(\sigma(g))\\ &= \frac{1}{|G|}\sum_{g\in G}\chi_\sigma(g)\\ &= \frac{1}{|G|}\sum_{g\in G}\mathrm{Fix}(g).\end{aligned}$$

620

因为 T 关于选定基的矩阵是单位块和零块的直和，所以有

$$\mathrm{tr}(T) = \dim(V^G),$$

而 $\mathrm{tr}(T)$ 是单位块的大小，即 $\dim(V^G)=N$. 所以，

$$N = \frac{1}{|G|}\sum_{g\in G}\mathrm{Fix}(g).$$

■

特征标表可以用于探察正规子群．

定义　如果 χ_τ 是由表示 $\tau: G\to \mathrm{GL}(V)$ 提供的特征标，则

$$\ker\chi_\tau = \ker\tau.$$

命题 8.138　设 $\theta=\chi_\tau$ 是由表示 $\tau: G\to\mathrm{GL}(V)$ 提供的有限群 G 的特征标．

（i）对每个 $g\in G$，有

$$|\theta(g)|\leqslant\theta(1).$$

（ii）

$$\ker\theta = \{g\in G : \theta(g)=\theta(1)\}.$$

（iii）如果 $\theta = \sum_j m_j\chi_j$，其中 m_j 是正整数，则

$$\ker\theta = \bigcap_j \ker\chi_j.$$

(iv) 如果 N 是 G 的正规子群，则存在不可约特征标 χ_{i_1}，…，χ_{i_s} 使得 $N = \bigcap_{j=1}^{s} \ker\chi_{i_j}$.

证明 (i) 根据拉格朗日定理，对每个 $g\in G$，$g^{|G|}=1$；由此 $\tau(g)$ 的特征值 $\varepsilon_1,\cdots,\varepsilon_d$ 是 $|G|$ 次单位根，其中 $d=\theta(1)$，从而对一切 j，$|\varepsilon_j|=1$. 根据C 中的三角不等式，

$$|\theta(g)| = \left|\sum_{j=1}^{d}\varepsilon_j\right| \leqslant d = \theta(1).$$

(ii) 如果 $g\in\ker\theta=\ker\tau$，则 $\tau(g)=I$，即单位矩阵，且 $\theta(g)=\operatorname{tr}(I)=\theta(1)$. 反之，假设 $\theta(g)=\theta(1)=d$；即 $\sum_{j=1}^{d}\varepsilon_j=d$. 根据命题 1.42，一切特征值 ε_j 相等，比如对一切 j，$\varepsilon_j=\omega$. 所以根据系 8.120 (iii)，$\tau(g)=\omega I$，从而

621

$$\theta(g)=\theta(1)\omega.$$

但根据假设，$\theta(g)=\theta(1)$，因此 $\omega=1$；即 $\tau(g)=I$ 和 $g\in\ker\tau$.

(iii) 对一切 $g\in G$，有

$$\theta(g)=\sum_j m_j\chi_j(g);$$

特别地，

$$\theta(1)=\sum_j m_j\chi_j(1).$$

如果 $g\in\ker\theta$，则 $\theta(g)=\theta(1)$. 假设有某个 j' 使得 $\chi_{j'}(g)\neq\chi_{j'}(1)$. 因 $\chi_{j'}(g)$是单位根的和，运用命题 1.42，必有 $|\chi_{j'}(g)|<\chi_{j'}(1)$，从而 $|\theta(g)|=\sum_j m_j|\chi_j(g)|<\sum_j\chi_j(1)=1$，这蕴涵 $\theta(g)\neq\theta(1)$,产生矛盾 . 所以 $g\in\bigcap_j\ker\chi_j$. 关于反包含，如果 $g\in\ker\chi_j$，则 $\chi_j(g)=\chi_j(1)$，从而

$$\theta(g)=\sum_j m_j\chi_j(g)=\sum_j m_j\chi_j(1)=\theta(1);$$

因此，$g\in\ker\theta$.

(iv) 只需求出 G 的一个表示以 N 为核 . 根据 (ii) 和例8.125(ii)，G/N 的正则表示 ρ 是忠实的 (即是一个单射)，因此它的核是 $\{1\}$. 如果 $\pi: G\to G/N$ 是自然映射，则 $\rho\pi$ 是 G 的以 N 为核的表示 . 如果 θ 是由 $\rho\pi$ 提供的特征标，则根据引理 8.126，$\theta=\sum_j m_j\chi_j$，其中 m_j 是正整数，因此用 (iii) 便得结果 . ■

例 8.139 本例中构造例 8.148 中 S_4 的特征标表 . 我们知道 $\ker\chi_2=A_4$ 和 $\ker\chi_3=\mathbf{V}$ 是 S_4 中仅有的两个正规子群 ($\{1\}$ 和 S_4 之外) . 此外，$\mathbf{V}\leqslant A_4$.

在例 8.140 中，我们知道 $\ker\chi_2=\{1\}\cup z^G\cup y^G$ (其中 z^G 表示 z 在 G 中的共轭类) 和 $\ker\chi_3=\{1\}\cup z^G\cup x^G$. 另一个正规子群是 $\ker\chi_2\cap\ker\chi_3=\{1\}\cup z^G$. ■

由特征标描述的正规子群是用共轭类的并给出的；这个观点可以给出 A_5 的单性的另一证明 . 在习题 2.89 (iv) 中，我们看到 A_5 有 5 个共轭类，大小是 1，12，12，15 和 20. 因每个正规子群包含幺元，所以 A_5 的正规子群的阶是这些数中某几个的和，而且总有 1. 但易知这样的和中只有 1 和 60 是 60 的因数，因此只有$\{1\}$和 A_5 自己是正规子群 .

有方法把商群的表示“提升”为这个群的表示 .

定义 设 $H\lhd G$，并设 $\sigma: G/H\to\mathrm{GL}(V)$ 是表示 . 如果 $\pi: G\to G/H$ 是自然映射，则表示

$\sigma\pi: G \to \mathrm{GL}(V)$ 叫做 σ 的**提升**.

622

给出 G 在$\mathbb{C}(G/H)$-模 V 上的标量乘法为对 $v \in V$,

$$gv = (gH)v.$$

于是，V 的每个$\mathbb{C}G$-子模也是$\mathbb{C}(G/H)$-子模；因此，如果 V 是单$\mathbb{C}(G/H)$-模，则它也是单$\mathbb{C}G$-模. 由此，如果 $\sigma: G/H \to \mathrm{GL}(V)$是 G/H 的不可约表示，则它的提升也是 G 的不可约表示.

例 8.140 我们知道 D_8 和 $\mathbf{Q}$ 是不同构的 8 阶非阿贝尔群，现在将证明它们有相同的特征标表.

如果 G 是一个 8 阶非阿贝尔群，则它的中心是 2 阶的，比如 $Z(G) = \langle z \rangle$. 现在根据习题 2.69，$G/Z(G)$ 不是循环群，因此 $G/Z(G) \cong \mathbf{V}$. 所以，如果 $\sigma: \mathbf{V} \to \mathbb{C}$ 是 $\mathbf{V}$ 的不可约表示，则它的提升 $\sigma\pi$ 是 G 的不可约表示. 这给出 G 的 4 个（必不可约）线性特征标，每一个在 z 上都取值 1. 由于 G 不是阿贝尔群，必有一个次数$n_5>1$的不可约特征标 χ_5（如果一切 $n_i=1$，则$\mathbb{C}G$ 是交换群，从而 G 是阿贝尔群）. 因 $\sum_i n_i^2 = 8$，可知 $n_5=2$. 于是有 5 个不可约表示，因此有 5 个共轭类；选取代表元 g_i 为 1，z，x，y，w. 表 8.4 是特征标表.

表 8.4　D_8 和 $\mathbf{Q}$ 的特征标表

g_i	1	z	x	y	w
h_i	1	1	2	2	2
χ_1	1	1	1	1	1
χ_2	1	1	-1	1	-1
χ_3	1	1	1	-1	-1
χ_4	1	1	-1	-1	1
χ_5	2	-2	0	0	0

χ_5 的值利用列的正交关系计算得到. 例如，如果特征标表的最后一行是

$$2\ a\ b\ c\ d,$$

则第 1 列和第 2 列的内积给出方程 $4+2a=0$，因此 $a=-2$. 读者可以验证 $0=b=c=d$. ■

正交关系有助于特征标表的计算，但显然对于提供特征标也是有用的. 一个重要的特征标类是由诱导表示提供的特征标所组成；即由群 G 的子群 H 的表示所确定的群 G 的表示.

623

属于弗罗贝尼乌斯的诱导表示的最初构造是十分复杂的. 张量积使得这个构造相当自然. 环$\mathbb{C}G$ 是一个$(\mathbb{C}G,\mathbb{C}H)$-双模（因为$\mathbb{C}H$ 是$\mathbb{C}G$ 的子环），因此，如果 V 是左$\mathbb{C}H$-模，则张量积$\mathbb{C}G \otimes_{\mathbb{C}H} V$ 有定义；引理 8.80 说这个张量积事实上是一个左$\mathbb{C}G$-模.

定义 设 H 是群 G 的子群. 如果 V 是左$\mathbb{C}H$-模，则**诱导模**是指左$\mathbb{C}G$-模

$$V\uparrow^G = \mathbb{C}G \otimes_{\mathbb{C}H} V.$$

对应的表示 $\rho\uparrow^G: G \to V^G$ 叫做**诱导表示**. 由 $\rho\uparrow^G$ 提供的 G 的特征标叫做**诱导特征标**，记为 $\chi_\rho\uparrow^G$.

首先我们认识到一个诱导表示的特征标未必局限于最初的子群表示. 例如，我们已经看到$A_3 \cong \mathbb{I}_3$ 的一个不可约特征标有复数值，而 S_3 的每个不可约特征标有（实）整数值. 与之相关的是两个元素在一个群中可以共轭，但在子群中不共轭（例如，A_3 中的非平凡元素在 S_3 中共轭，这是因为它们有相同的轮换结构，但在阿贝尔群 A_3 中它们不共轭）.

下一引理将帮助我们计算由诱导表示提供的特征标.

引理 8.141 （i）如果 $H \leqslant G$，则$\mathbb{C}G$ 是 $[G:H]$ 个生成元上的自由右$\mathbb{C}H$-模.

（ii）如果左 $\mathbb{C}H$-模 V 有一个（向量空间）基 $e_1,\cdots,e_m$，则诱导模 $V\uparrow^G = \mathbb{C}G \otimes_{\mathbb{C}H} V$ 的一个（向量空间）基是一切 $t_i \otimes e_j$ 的族，其中 $t_1,\cdots,t_n$ 是 H 在 G 中的陪集代表系.

证明 （i）因 $t_1,\cdots,t_n$ 是 H 在 G 中的陪集代表系（当然，$n=[G:H]$），我们知道 G 是不相交并

$$G = \bigcup_i t_i H;$$

于是，对每个 $g\in G$，存在唯一的 i 和唯一的 $h\in H$ 使得 $g=t_ih$．我们断言 $t_1,\cdots,t_n$ 是$\mathbb{C}G$的看作右$\mathbb{C}H$-模的基．

如果 $u\in\mathbb{C}G$，则 $u=\sum_g a_g g$，其中 $a_g\in\mathbb{C}$．把每个项重写得

$$a_g g=a_g t_i h=t_i a_g h$$

624 （$\mathbb{C}$中的标量和每一个都能交换），把包含同一 t_i 的项归并起来，得到 $u=\sum_i t_i\eta_i$，其中$\eta_i\in\mathbb{C}H$.

为证明这个表达式的唯一性，假设 $0=\sum_i t_i\eta_i$，其中 $\eta_i\in\mathbb{C}H$．现在 $\eta_i=\sum_{h\in H}a_{ih}h$，其中 $a_{ih}\in\mathbb{C}$．用它替换得

$$0=\sum_{i,h}a_{ih}t_ih.$$

但 $t_ih=t_jh'$ 当且仅当 $i=j$ 和 $h=h'$，因此 $0=\sum_{i,h}a_{ih}t_ih=\sum_{g\in G}a_{ih}g$，其中 $g=t_ih$．因 G 的元素是$\mathbb{C}G$ 的基（看作$\mathbb{C}$上的向量空间），对一切 i，h 有 $a_{ih}=0$.

（ⅱ）根据定理 8.87,

$$\mathbb{C}G\otimes_{\mathbb{C}H}V\cong\sum_i t_i\,\mathbb{C}H\otimes_{\mathbb{C}H}V.$$

由此每个 $u\in\mathbb{C}G\otimes_{\mathbb{C}H}V$ 有作为 $t_i\otimes e_j$ 的$\mathbb{C}$-线性组合的唯一表达式，因此这些元素组成一个基．■

我们引入下面的记号．如果 $H\leqslant G$ 和 $\chi:H\to\mathbb{C}$ 是函数，则 $\dot{\chi}:G\to\mathbb{C}$ 由下式给出：

$$\dot{\chi}(g)=\begin{cases}0 & \text{当 } g\notin H\\ \chi(g) & \text{当 } g\in H.\end{cases}$$

定理 8.142 *如果 χ_σ 是由群 G 的子群 H 的表示 $\sigma:H\to\mathrm{GL}(V)$ 提供的特征标，则诱导特征标 $\chi_\sigma\uparrow^G$ 由下式给出：*

$$\chi_\sigma\uparrow^G(g)=\frac{1}{|H|}\sum_{a\in G}\dot{\chi}_\sigma(a^{-1}ga).$$

证明 设 $t_1,\cdots,t_n$ 是 H 在 G 中的陪集代表系，因此 G 是不相交并 $G=\bigcup_i t_iH$，设 $e_1,\cdots,e_m$ 是 V 的（向量空间）基．根据引理8.141(ⅱ)，向量空间 $V^G=\mathbb{C}G\otimes_{\mathbb{C}H}V$ 的基由一切 $t_i\otimes e_j$ 组成．注意

$$gt_i=t_{k(i)}h_i,$$

其中 $h_i\in H$，因此

$$\begin{aligned}g(t_i\otimes e_j)&=(gt_i)\otimes e_j\\&=t_{k(i)}h_i\otimes e_j\\&=t_{k(i)}\otimes\sigma(h_i)e_j\end{aligned}$$

（最后一个等式成立是因为可以把 H 中的任一元素移到张量记号的另一边）．现在 $g(t_i\otimes e_j)$ 写作 V^G的一切基元素的$\mathbb{C}$-线性组合，这是因为对 $p\neq k(i)$，$t_p\otimes e_j$ 的系数都是 0. 因此，$\sigma\uparrow^G(g)$ 给出 $nm\times nm$ 矩阵，对固定的 i，以 $t_i\otimes e_j$ 加标的 m 个列除了一个 $m\times m$ 块等于

625

$$[a_{pq}(h_i)]=[a_{pq}(t_{k(i)}^{-1}gt_i)]$$

之外全等于 0. 于是，大矩阵分成 $m\times m$ 的块，它们中的大多数是 0，在大矩阵的对角线上的一个块非零当且仅当 $k(i)=i$；即

$$t_{k(i)}^{-1}gt_i=t_i^{-1}gt_i=h_i\in H.$$

诱导特征标是大矩阵的迹，它是对角线上的那些块的迹之和．所以，

$$\chi_\sigma\uparrow^G(g)=\sum_{t_i^{-1}gt_i\in H}\operatorname{tr}([a_{pq}(t_i^{-1}gt_i)])$$
$$=\sum_i\dot{\chi}_\sigma(t_i^{-1}gt_i)$$

（记住 $\dot{\chi}_\sigma$ 在 H 之外是 0）．现在重写直和项（为了得到不依赖于陪集代表系取法的公式）：如果 $t_i^{-1}gt_i\in H$，则 $(t_ih)^{-1}g(t_ih)=h^{-1}(t_i^{-1}gt_i)h$ 在 H 中，由于 χ_σ 是 H 上的类函数，因此对固定的 i，

$$\sum_{h\in H}\dot{\chi}_\sigma((t_ih)^{-1}g(t_ih))=|H|\,\dot{\chi}_\sigma(t_i^{-1}gt_i),$$

所以

$$\chi_\sigma\uparrow^G(g)=\sum_i\dot{\chi}_\sigma(t_i^{-1}gt_i)$$
$$=\frac{1}{|H|}\sum_{i,h}\dot{\chi}_\sigma((t_ih)^{-1}g(t_ih))$$
$$=\frac{1}{|H|}\sum_{a\in G}\dot{\chi}_\sigma(a^{-1}ga).$$ ■

注　我们已经讨论了诱导特征标，但容易把这个讨论推广到**诱导类函数**．如果 $H\leqslant G$，则 H 上的一个类函数 θ 有作为 H 的不可约特征标的 $\mathbb{C}$－线性组合的唯一表达式，比如 $\theta=\sum c_i\chi_i$，因此可以定义

$$\theta\uparrow^G=\sum c_i\chi_i\uparrow^G.$$

易知 $\theta\uparrow^G$ 是 G 上的类函数，且定理 8.142 中的公式可以扩张到诱导类函数．

如果对 $h\in H$，$\sigma(h)$ 的矩阵（关于 V 的基 $e_1,\cdots,e_m$）是 $B(h)$，则对一切 $g\in G$，定义 $m\times m$ 矩阵 $\dot{B}(g)$ 为

$$\dot{B}(g)=\begin{cases}0 & \text{如果 } g\notin H;\\ B(g) & \text{如果 } g\in H.\end{cases}$$

626

定理 8.142 的证明使得可以把诱导表示的矩阵写成分块矩阵的形式：

$$\sigma\uparrow^G(g)=\begin{bmatrix}\dot{B}(t_1^{-1}gt_1) & \dot{B}(t_1^{-1}gt_2) & \cdots & \dot{B}(t_1^{-1}gt_n)\\ \dot{B}(t_2^{-1}gt_1) & \dot{B}(t_2^{-1}gt_2) & \cdots & \dot{B}(t_2^{-1}gt_n)\\ \vdots & \vdots & \vdots & \vdots\\ \dot{B}(t_n^{-1}gt_1) & \dot{B}(t_n^{-1}gt_2) & \cdots & \dot{B}(t_n^{-1}gt_n)\end{bmatrix}.$$

系 8.143　设 H 是有限群 G 的子群，并设 χ 是 H 上的特征标．

（ⅰ）$\chi\uparrow^G(1)=[G:H]\chi(1)$．

（ⅱ）如果 $H\lhd G$，则对一切 $g\notin H$，$\chi\uparrow^G(g)=0$.

证明　（ⅰ）对一切 $a\in G$，有 $a^{-1}1a=1$，因此在和 $\chi\uparrow^G(1)=\frac{1}{|H|}\sum_{a\in G}\dot{\chi}(a^{-1}ga)$ 中有 $|G|$ 个项等于 $\chi(1)$；从而，

$$\chi\uparrow^G(1)=\frac{|G|}{|H|}\chi(1)=[G:H]\chi(1).$$

（ⅱ）如果 $H \lhd G$，则对一切 $a \in G, g \notin H$ 蕴涵 $a^{-1}ga \notin H$．所以对一切 $a \in G, \dot{\chi}(a^{-1}ga) = 0$，因此 $\chi\uparrow^G(g) = 0$． ■

例 8.144 设 $H \leqslant G$ 是指数为 n 的子群，设 $X = \{t_1H, \cdots, t_nH\}$ 是 H 的左陪集的族，并设 $\varphi: G \to S_X$ 是 G 在 H 的陪集上的（置换）表示．和例8.123（ⅴ）一样，可以认为 $\varphi: G \to \mathrm{GL}(V)$，其中 V 是$\mathbb{C}$上以 X 为基的向量空间；即 φ 是本节意义下的表示．

我们断言，如果 χ_φ 是由 φ 提供的特征标，则 $\chi_\varphi = \epsilon\uparrow^G$，其中 ϵ 是 H 上的平凡特征标．一方面，例 8.123（ⅴ）证明对每个 $g \in G$，

$$\chi_\varphi(g) = \mathrm{Fix}(\varphi(g)).$$

另一方面，假定 $\varphi(g)$ 是置换（写成两行的记号）

$$\varphi(g) = \begin{pmatrix} t_1H & \cdots & t_nH \\ gt_1H & \cdots & gt_nH \end{pmatrix}.$$

现在 $gt_iH = t_iH$ 当且仅当 $t_i^{-1}gt_i \in H$．于是，$\dot{\epsilon}(t_i^{-1}gt_i) \neq 0$ 当且仅当 $gt_iH = t_iH$，因此

627

$$\epsilon\uparrow^G(g) = \mathrm{Fix}(\varphi(g)).$$ ■

即使子群 H 的一个特征标 λ 是不可约的，它的诱导特征标也未必不可约．例如，设 $G = S_3$，H 是由（1 2）生成的循环子群．线性表示 $\sigma = \mathrm{sgn}: H \to \mathbb{C}$ 是不可约的，它提供的特征标 χ_σ 使得

$$\chi_\sigma(1) = 1 \text{ 和 } \chi_\sigma((1\ 2)) = -1.$$

运用诱导特征标的公式，可求得

$$\chi_\sigma\uparrow^{S_3}(1) = 3, \chi_\sigma\uparrow^{S_3}((1\ 2)) = -1 \text{ 和 } \chi_\sigma\uparrow^{S_3}((1\ 2\ 3)) = 0.$$

因为 $(\chi_\sigma\uparrow^{S_3}, \chi_\sigma\uparrow^{S_3}) = 2$，系 8.130 表明 $\chi_\sigma\uparrow^{S_3}$ 不是不可约的．易知 $\chi_\sigma\uparrow^{S_3} = \chi_2 + \chi_3$，后面一个是 S_3 的非平凡不可约特征标．

我们必须提到布饶尔（R. Brauer）的一个结果．有限群 G 的一个子群 E 称为**初等的**，如果 $E = Z \times P$，其中 Z 是循环群，P 是 p-群，其中 p 是某个素数．

定理（布饶尔） 有限群 G 上的每个复特征标 θ 都有

$$\theta = \sum_i m_i\mu_i\uparrow^G$$

的形式，其中 $m_i \in \mathbb{Z}$，μ_i 是 G 的初等子群上的线性特征标．

证明 见 Curtis-Reiner 所著的《Theory of Finite Groups and Associative Algebras》，283 页． ■

定义 如果 H 是群 G 的子群，则每个表示 $\sigma: G \to \mathrm{GL}(V)$ 用限制给出表示 $\sigma | H: H \to \mathrm{GL}(V)$．（用模来说，每个左$\mathbb{C}G$-模 V 可以看作一个左$\mathbb{C}H$-模．）我们称 $\sigma | H$ 为 σ 的**限制**，并把它记为$\sigma\downarrow_H$．由 $\sigma\downarrow_H$ 提供的 H 的特征标记为 $\chi_\sigma\downarrow_H$．

下一结果呈示了群 G 的特征标和子群的特征标之间的重要关系．（形式上类似于伴随同构．）

定理 8.145（弗罗贝尼乌斯互反性） 设 H 是群 G 的子群，设 χ 是 G 上的一个类函数，并设 θ 是 H 上的类函数，则

$$(\theta\uparrow^G, \chi)_G = (\theta, \chi\downarrow_H)_H,$$

628

其中 $(\ ,\ )_G$ 表示 $\mathrm{cf}(G)$ 上的内积，$(\ ,\ )_H$ 表示 $\mathrm{cf}(H)$ 上的内积．

证明

$$\begin{aligned}(\theta\uparrow^G,\chi)_G &= \frac{1}{|G|}\sum_{g\in G}\theta\uparrow^G(g)\,\overline{\chi(g)}\\ &= \frac{1}{|G|}\sum_{g\in G}\frac{1}{|H|}\sum_{a\in G}\dot{\theta}(a^{-1}ga)\,\overline{\chi(g)}\\ &= \frac{1}{|G|}\frac{1}{|H|}\sum_{a,g\in G}\dot{\theta}(a^{-1}ga)\,\overline{\chi(a^{-1}ga)},\end{aligned}$$

最后一个等式的导出是因为 χ 是类函数. 对固定的 $a\in G$，当 g 遍历 G 时，$a^{-1}ga$ 也遍历 G. 所以记 $x=a^{-1}ga$，于是上面的等式继续有

$$\begin{aligned}&= \frac{1}{|G|}\frac{1}{|H|}\sum_{a,x\in G}\dot{\theta}(x)\,\overline{\chi(x)}\\ &= \frac{1}{|G|}\frac{1}{|H|}\sum_{a\in G}\Big(\sum_{x\in G}\dot{\theta}(x)\,\overline{\chi(x)}\Big)\\ &= \frac{1}{|G|}\frac{1}{|H|}\,|G|\,\sum_{x\in G}\dot{\theta}(x)\,\overline{\chi(x)}\\ &= \frac{1}{|H|}\sum_{x\in G}\dot{\theta}(x)\,\overline{\chi(x)}\\ &= (\theta,\chi\downarrow_H)_H,\end{aligned}$$

倒数第二个等式成立是因为 $\dot{\theta}(x)$ 把子群 H 变成零. ■

下面的初等注记便于诱导类函数的计算.

引理 8.146 *设 H 是有限群 G 的子群，并设 χ 是 H 上的类函数，则*

$$\chi\uparrow^G(g) = \frac{1}{|H|}\sum_i |C_G(g_i)|\,\dot{\chi}(g_i^{-1}gg_i).$$

证明　设 $|C_G(g_i)|=m_i$. 如果 $a_0^{-1}g_ia_0=g$，我们断言恰有 m_i 个元素 $a\in G$ 使得 $a^{-1}g_ia=g$. G 中至少有 m_i 个元素构成 g_i 和 g 共轭，就是一切满足 $a\in C_G(g_i)$ 的 aa_0. 这样的元素至多也只有 m_i 个，因为如果 $b^{-1}g_ib=g$，则 $b^{-1}g_ib=a_0^{-1}g_ia_0$，从而 $a_0b\in C_G(g_i)$. 现在通过合并 $\chi\uparrow^G(g)$ 的公式中含有 g_i 的项便得到结果. ■

例 8.147　表 8.5 是 A_4 的特征标表，其中 $\omega=e^{2\pi i/3}$ 是三次单位原根.

629

表 8.5　A_4 的特征标表

g_i	(1)	(1 2 3)	(1 3 2)	(1 2) (3 4)
h_i	1	4	4	3
χ_1	1	1	1	1
χ_2	1	ω	ω^2	1
χ_3	1	ω^2	ω	1
χ_4	3	0	0	−1

群 A_4 由恒等置换、8 个 3-轮换和 3 个不相交对换的乘积组成. 在 S_4 中，一切 3-轮换都共轭；如果 $g=(1\ 2\ 3)$，则 $[S_4:C_{S_4}(g)]=8$. 由此，$|C_{S_4}(g)|=3$，从而 $C_{S_4}(g)=\langle g\rangle$. 所以在 A_4 中 g 的共轭的个数是 $[A_4:C_{A_4}(g)]=4$[我们知道 $C_{A_4}(g)=A_4\cap C_{S_4}(g)=\langle g\rangle$]. 读者可以证明 g 和 g^{-1} 是不共轭的，因此我们已经验证了特征标表的前两行.

χ_2 和 χ_3 的行是 $A_4/\mathbf{V}\cong \mathbb{I}_3$ 的线性特征标的提升. 注意，因为 $\mathbf{V}$ 是提升表示的核，所以如果 $h=(1\ 2)(3\ 4)$，则 $\chi_2(h)=\chi_2(1)=1$；同样，$\chi_3(h)=1$. 现在因为 $3+(n_4)^2=12$，所以 $\chi_4(1)=3$. 表底一行由列的正交性得到.（我们可以用系 8.130 验证 3 次特征标是不可约的.） ■

例 8.148　表 8.6 是 S_4 的特征标表.

我们知道对一切 n，S_n 中的两个置换共轭当且仅当它们有相同的轮换结构；例2.5（ⅰ）中计算了 S_4 中共轭类的大小．

表 8.6　S_4 的特征标表

g_i	(1)	(1 2)	(1 2 3)	(1 2 3 4)	(1 2)(3 4)
h_i	1	6	8	6	3
χ_1	1	1	1	1	1
χ_2	1	−1	1	−1	1
χ_3	2	0	−1	0	2
χ_4	3	1	0	−1	−1
χ_5	3	−1	0	1	−1

χ_2 和 χ_3 的行是 $S_4/\mathbf{V}\cong S_3$ 的不可约特征标的提升．这两行第4列的元素来自 $(1\ 2)\mathbf{V}=(1\ 2\ 3\ 4)\mathbf{V}$；这两行最后一列的元素来自 $\mathbf{V}$ 是核（在每种情形中），从而对 $j=2,3,\chi_j(1\ 2)(3\ 4)=\chi_j(1)$．

我们用 $24=1+1+4+n_4^2+n_5^2$ 完成第1列；这样，$n_4=3=n_5$．我们来看 χ_4 是否一个诱导特征标；如果它是诱导特征标，则系8.143（ⅰ）证明它是由指数为3的子群 H 的线性特征标产生的．这样的子群是8阶的，从而它是一个西罗2-子群；即 $H\cong D_8$．选取一个这样的子群：设

630

$$H=\langle\mathbf{V},(1\ 3)\rangle=\mathbf{V}\cup\{(1\ 3),(2\ 4),(1\ 2\ 3\ 4),(1\ 4\ 3\ 2)\}.$$

共轭类是

$$C_1=\{1\};$$
$$C_2=\{(1\ 3)(2\ 4)\};$$
$$C_3=\{(1\ 2)(3\ 4),(1\ 4)(2\ 3)\};$$
$$C_4=\{(1\ 3),(2\ 4)\};$$
$$C_5=\{(1\ 2\ 3\ 4),(1\ 4\ 3\ 2)\}.$$

设 θ 是由

C_1	C_2	C_3	C_4	C_5
1	1	−1	1	−1

定义的 H 上的特征标．

定义 $\chi_4=\theta^{S_4}$．用诱导特征标的公式，并借助于引理8.146，可以得到这个特征标表的第4行．然而在进行到第5行之前，我们看到系8.130证明 χ_4 是不可约的，这是因为 $(\chi_4,\chi_4)=1$．最后，正交关系使得可以计算第5行．■

在此，我们必须引入代数整数．因 G 是有限群，拉格朗日定理给出对一切 $g\in G,g^{|G|}=1$．由此，如果 $\sigma:G\to\mathrm{GL}(V)$ 是表示，则对一切 $g,\sigma(g)^{|G|}=I$；因此，$\sigma(g)$ 的一切特征值都是 $|G|$ 次单位根，从而一切特征值都是代数整数．根据命题7.24，$\sigma(g)$ 的迹是特征值的和，也是代数整数．

我们现在能够证明下面的重要结果．

定理 8.149　*有限群 G 的不可约特征标的次数 n_i 是 $|G|$ 的因数．*

证明　根据系3.44，有理数 $\alpha=|G|/n_i$ 如果也是一个代数整数，则必是一个整数．现在系8.10（ⅱ）说，如果存在一个忠实 $\mathbb{Z}[\alpha]$-模 M，它又是一个有限生成阿贝尔群，则 α 是代数整数，其中 $\mathbb{Z}[\alpha]$ 是 $\mathbb{C}$ 的包含 α 的最小子环．

根据命题8.128，有

$$e_i=\sum_{g\in G}\frac{n_i}{|G|}\chi_i(g^{-1})g$$
$$=\sum_{g\in G}\frac{1}{\alpha}\chi_i(g^{-1})g.$$

631

因此，$\alpha e_i = \sum_{g\in G}\chi_i(g^{-1})g$. 但 e_i 是幂等元：$e_i^2=e_i$，从而

$$\alpha e_i = \sum_{g\in G}\chi_i(g^{-1})ge_i.$$

定义 M 为一切形如 ζge_i 的元素生成的$\mathbb{C}G$的阿贝尔子群，其中 ζ 是 $|G|$ 次单位根，$g\in G$；当然，M 是有限生成阿贝尔群.

为证明 M 是$\mathbb{Z}[\alpha]$-模，只需证明 $\alpha M\subseteq M$. 但

$$\begin{aligned}\alpha\zeta ge_i &= \zeta g\alpha e_i\\ &= \zeta g\sum_{h\in G}\chi_i(h^{-1})he_i\\ &= \sum_{h\in G}\chi_i(h^{-1})\zeta ghe_i.\end{aligned}$$

然而，因为 $\chi_i(h^{-1})$ 是 $|G|$ 次单位根的和，所以最后那个元素在 M 中.

最后，如果 $\beta\in\mathbb{C}$ 和 $u\in\mathbb{C}G$，则 $\beta u=0$ 当且仅当 $\beta=0$ 或 $u=0$. 然而，$\mathbb{Z}[\alpha]\subseteq\mathbb{C}$ 和 $M\subseteq\mathbb{C}G$，因此正如所要的 M 是一个忠实 $\mathbb{Z}[\alpha]$-模. ■

下一节我们要提出特征标理论的两个重要应用；对于其他应用以及表示论的更严密的研究，有兴趣的读者应该阅读柯蒂斯-赖纳、费特（Feit）、Huppert 和艾萨克斯（Isaacs）的书. 表示论是 20 世纪 80 年代证明有限单群分类的一个要素：有几个无限族和属于非无限族的 26 个零星群（见 Kostrikin 和 Shafarevich 编的书中 R. Carter 写的一章和 Gorenstein-Lyons-Solomon 所著的《The Classification of the Finite Simple Groups》). 康伟（Conway）等人的 ATLAS，包含 10^{25} 阶以下每个单群的特征标表，以及一切零星群的特征标表. 最大的零星单群叫做怪物，它的阶为

$$2^{46}\cdot 3^{20}\cdot 5^{9}\cdot 7^{6}\cdot 11^{2}\cdot 13^{3}\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 41\cdot 47\cdot 59\cdot 71.$$

习题

8.55　证明：如果 θ 是有限群 G 的广义特征标，则存在特征标 χ 和 ψ 使得 $\theta=\chi-\psi$.

8.56　（i）证明：如果 z 是单位复根，则 $z^{-1}=\overline{z}$.

（ii）证明：如果 G 是有限群，$\sigma: G\to \mathrm{GL}(V)$ 是表示，则对一切 $g\in G$，

$$\chi_\sigma(g^{-1})=\overline{\chi_\sigma(g)}.$$

提示：用 $\sigma(g)$ 的每个特征值都是单位根的事实以及下列事实：如果 A 是域 k 上的非奇异矩阵且 $u_1,\cdots,u_n$ 是 A 的特征值（带有重数），则 A^{-1} 的特征值是 $u_1^{-1},\cdots,u_n^{-1}$；即 $\overline{u}_1,\cdots,\overline{u}_n$.　632

8.57　如果 $\sigma: G\to\mathrm{GL}(n,\mathbb{C})$ 是表示，它的**逆步表示** $\sigma^*: G\to\mathrm{GL}(n,\mathbb{C})$ 是由

$$\sigma^*(g)=\sigma(g^{-1})^t$$

给出的函数，其中^t 表示转置.

（i）证明表示 σ 的逆步表示也是表示，当 σ 不可约时，它也不可约.

（ii）证明由逆步表示 σ^* 提供的特征标 χ_{σ^*} 是

$$\chi_{\sigma^*}(g)=\overline{\chi_\sigma(g)},$$

其中 $\overline{\chi_\sigma(g)}$ 是复共轭. 由此推出，如果 χ 是 G 的特征标，则 $\overline{\chi}$ 也是特征标.

8.58　构造 S_3 的一个 2 次不可约表示.

8.59　（i）如果 $g\in G$，其中 G 是有限群，证明 g 和 g^{-1} 共轭当且仅当对 G 的每个特征标 χ，$\chi(g)$ 是实数.

（ii）证明 S_n 的每个特征标都是实值函数.（弗罗贝尼乌斯有一个定理说 S_n 的每个特征标都取整数值.）

8.60 (i) 如果G是有限阿贝尔群，定义它的**特征标群**G^*为

$$G^* = \mathrm{Hom}(G, \mathbb{C}^\times),$$

其中$\mathbb{C}^\times$是非零复数的乘法群．证明$G^* \cong G$.

提示：用有限阿贝尔群的基本定理．

(ii) 证明：当G是有限阿贝尔群时，$\mathrm{Hom}(G,\mathbb{C}^\times) \cong \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z})$.

(iii) 证明有限阿贝尔群的每个不可约特征标都是线性的.

8.61 证明一个单群只有线性特征标是平凡特征标．由此推出，如果χ_i不是平凡特征标，则$n_i = \chi_i(1) > 1$.

8.62 设$\theta = \chi_\sigma$是由有限群G的表示σ提供的特征标．

(i) 如果$g \in G$，证明$|\theta(g)| = \theta(1)$当且仅当$\sigma(g)$是标量矩阵．

提示：用命题1.42.

(ii) 如果θ是不可约特征标，证明

$$Z(G/\ker\theta) = \{g \in G : |\theta(g)| = \theta(1)\}.$$

8.63 如果G是有限群，证明它的（必不可约）线性表示的个数是$[G:G']$.

8.64 设G是有限群．

(i) 如果$g \in G$，证明$|C_G(g)| = \sum_{i=1}^{r} |\chi_i(g)|^2$．由此可知$G$的特征标表给出$|C_G(g)|$.

(ii) 说明如何用G的特征标表确定G是否是阿贝尔群．

(iii) 说明如何用G的特征标表求G的正规子群的格以及它们的阶．

(iv) 如果G是有限群，说明如何用它的特征标表求换位子群G'.

提示：如果$K \lhd G$，则G/K的特征标表是G的特征标表的子矩阵，因此可以求G的有最大阶的阿贝尔商群．

633

(v) 说明如何用有限群G的特征标表确定G是否可解．

8.65 (i) 说明如何用G的特征标表求$|Z(G)|$.

(ii) 说明如何用有限群G的特征标表确定G是否幂零．

8.66 回忆四元数群$\mathbf{Q}$有表现

$$\mathbf{Q} = (A, B \mid A^4 = 1, A^2 = B^2, BAB^{-1} = A^{-1}).$$

(i) 证明有表示$\sigma: \mathbf{Q} \to \mathrm{GL}(2,\mathbb{C})$使得

$$A \mapsto \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \text{和 } B \mapsto \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

(ii) 证明σ是一个不可约表示．

8.67 (i) 如果$\sigma: G \to \mathrm{GL}(V)$和$\tau: G \to \mathrm{GL}(W)$都是表示，证明由

$$(\sigma \otimes \tau)(g) = \sigma(g) \otimes \tau(g)$$

定义的

$$\sigma \otimes \tau : G \to \mathrm{GL}(V \otimes W)$$

是一个表示．

(ii) 证明由$\sigma \otimes \tau$提供的特征标是点态积：

$$\chi_\sigma \chi_\tau : g \mapsto \mathrm{tr}(\sigma(g))\mathrm{tr}(\tau(g)).$$

(iii) 证明$\mathrm{cf}(G)$是交换环（通常称为G的**伯恩赛德环**）．

8.6 伯恩赛德定理和弗罗贝尼乌斯定理

本节将用特征标理论证明群论中两个重要结果：伯恩赛德的$p^m q^n$定理和弗罗贝尼乌斯定理．

我们先给出下面舒尔引理的变种.

命题 8.150　*如果 $\sigma: G\to GL(V)$ 是不可约表示，且有一个线性变换 $\varphi: V\to V$ 对一切 $g\in G$ 满足*

$$\varphi\sigma(g)=\sigma(g)\varphi,$$

则 φ 是标量变换：存在 $\alpha\in\mathbb{C}$ 使得 $\varphi=\alpha 1_V$.

634

证明　向量空间 V 是 $\mathbb{C}G$-模，它的标量乘法为对一切 $v\in V, gv=\sigma(g)(v)$，对一切 $g\in G$ 满足等式 $\theta\sigma(g)=\sigma(g)\theta$ 的线性变换 θ 是 $\mathbb{C}G$-映射 $V^\sigma\to V^\sigma$. 因 σ 是不可约的，$\mathbb{C}G$-模 V^σ 是单的；根据舒尔引理［定理8.52(ⅱ)］，$\mathrm{End}(V^\sigma)$ 是除环，因此其中的每个非零元素是非奇异的. 现在对每个 $\alpha\in\mathbb{C}, \varphi-\alpha 1_V\in\mathrm{End}(V^\sigma)$；特别是当 α 是 φ 的特征值（它在 $\mathbb{C}$ 中，因为 $\mathbb{C}$ 是代数闭域）时也是这样. 特征值的定义说 $\varphi-\alpha 1_V$ 是奇异的，因此它必是 0；即正如所要证明的，$\varphi=\alpha 1_V$. ■

和命题8.119(ⅱ)一样，我们可以把由极小左理想 L_i 上的左乘给出的不可约表示 $\lambda_i: G\to GL(L_i)$ 看作 $\mathbb{C}$-代数映射 $\widetilde{\lambda}_i: \mathbb{C}G\to\mathrm{End}(L_i)$（毕竟，$\mathrm{im}\widetilde{\lambda}_i\subseteq\mathrm{End}(L_i)$）. 因此限制到 $\mathbb{C}G$ 的中心也是一个代数映射：

$$\widetilde{\lambda}_i: Z(\mathbb{C}G)\to\mathrm{End}(L_i)\cong\mathrm{Mat}_{n_i}(\mathbb{C}).$$

于是对每个 $z\in Z(\mathbb{C}G), \widetilde{\lambda}_i(z)$ 是一个 $n_i\times n_i$ 复矩阵. 根据命题 8.150，对每个 $z\in Z(\mathbb{C}G), \widetilde{\lambda}_i(z)$ 是一个标量矩阵：

$$\widetilde{\lambda}_i(z)=\omega_i(z)I,$$

其中 $\omega_i(z)\in\mathbb{C}$. 此外，因为 $\widetilde{\lambda}_i$ 是 $\mathbb{C}$-代数映射，所以函数 $\omega_i: Z(\mathbb{C}G)\to\mathbb{C}$ 也是 $\mathbb{C}$-代数映射.

回忆引理 8.68，$Z(\mathbb{C}G)$ 的基由类和

$$z_i=\sum_{g\in C_i}g$$

组成，其中 G 的共轭类是 $C_1, \cdots, C_r$.

命题 8.151　*设 $z_1,\cdots,z_r$ 是有限群 G 的类和.*

(ⅰ) 对每个 i，j，有

$$\omega_i(z_j)=\frac{h_j\chi_i(g_j)}{n_i},$$

其中 $g_j\in C_j$.

(ⅱ) 存在非负整数 $a_{ij\nu}$ 使得

$$z_iz_j=\sum_\nu a_{ij\nu}z_\nu.$$

(ⅲ) 复数 $\omega_i(z_j)$ 是代数整数.

635

证明　(ⅰ) 计算 $\widetilde{\lambda}_i(z_j)=\omega_i(z_j)I$ 的迹，因为 χ_i 在共轭类 C_j 上是常数，所以得到

$$n_i\omega_i(z_j)=\chi_i(z_j)=\sum_{g\in C_j}\chi_i(g)=h_j\chi_i(g_j),$$

所以 $\omega_i(z_j)=h_j\chi_i(g_j)/n_i$.

(ⅱ) 选取 $g_\nu\in C_\nu$. 群代数中乘法的定义表明 g_ν 在 z_iz_j 中的系数是

$$|\{(g_i,g_j)\in C_i\times C_j: g_ig_j=g_\nu\}|,$$

它是有限集的基数，因此是非负整数. 由于 z_ν 的一切系数都相等［因为我们在 $Z(\mathbb{C}G)$ 中］，因此这个数是 $a_{ij\nu}$.

(ⅲ) 设 M 是由一切 $\omega_i(z_j)$(其中 $j=1,\cdots,r$) 生成的 $\mathbb{C}$ 的（加法）子群．因 ω_i 是代数映射，

$$\omega_i(z_j)\omega_i(z_\ell)=\sum_{\nu}a_{j\ell\nu}\omega_i(z_\nu),$$

从而 M 是环，它作为阿贝尔群是有限生成的（因为 $a_{ij\nu}\in\mathbb{Z}$）．因此对每个 j，M 是 $\mathbb{Z}[\omega_i(z_j)]$－模，又是有限生成阿贝尔群．如果 M 是忠实的，则系8.10(ⅱ)给出 $\omega_i(z_j)$ 是代数整数．但 $M\subseteq\mathbb{C}$，从而非零元素的积非零，这蕴涵 M 是忠实 $\mathbb{Z}[\omega_i(z_j)]$－模． ■

完成伯恩赛德定理的证明几乎准备就绪．

命题 8.152 *如果有某个 i，j 使得 $(n_i,h_j)=1$，则 $|\chi_i(g_j)|=n_i$ 或 $\chi_i(g_j)=0$.*

证明 根据假设，存在 $\mathbb{Z}$ 中整数 s 和 t 使得 $sn_i+th_j=1$，从而对 $g_j\in C_j$ 有

$$\frac{\chi_i(g_j)}{n_i}=s\chi_i(g_j)+\frac{th_j\,\chi_i(g_j)}{n_i}.$$

因此，命题8.151(ⅲ)给出 $\chi_i(g_j)/n_i$ 是代数整数，从而根据命题8.138(ⅰ)，$|\chi_i(g_j)|\leqslant n_i$；于是只需证明：如果 $|\chi_i(g_j)/n_i|<1$，则 $\chi_i(g_j)=0$.

设 $m(x)\in\mathbb{Z}[x]$ 是 $\alpha=\chi_i(g_j)/n_i$ 的极小多项式；即 $m(x)$ 是 $\mathbb{Z}[x]$ 中以 α 为根、次数最小的首一多项式．在系 6.29 中我们证明了 $m(x)$ 是 $\mathbb{Q}[x]$ 中的不可约多项式．如果 α' 是 $m(x)$ 的根，则命题4.13 证明有某个 $\sigma\in\mathrm{Gal}(E/\mathbb{Q})$ 使得 $\alpha'=\sigma(\alpha)$，其中 $E/\mathbb{Q}$ 是 $m(x)(x^{|G|}-1)$ 的分裂域．但

$$\alpha=\frac{1}{n_i}(\varepsilon_1+\cdots+\varepsilon_{n_i}),$$

其中各个 ε 是 $|G|$ 次单位根，因为 $\alpha'=\sigma(\alpha)$ 也是这样的和．由此，$|\alpha'|\leqslant 1$［如同命题8.138(ⅰ)的证明］．所以，如果 $N(\alpha)$ 是 α 的范数（根据定义它是 $m(x)$ 的一切根之积的绝对值），则 $N(\alpha)<1$（因为我们假定 $|\alpha|<1$）．但 $N(\alpha)$ 是 $m(x)$ 的常数项的绝对值，它是一个整数．所以，$N(\alpha)=0$，因此 $\alpha=0$，从而正如所要的 $\chi_i(g_j)=0$． ■

636

最后，我们可以证明上一节开始时命题 8.116 的假设．

定理 8.153 *如果 G 是非阿贝尔的有限单群，则 $\{1\}$ 是大小为素数幂的唯一共轭类．所以伯恩赛德定理成立：每个 p^mq^n 阶群都是可解的，其中 p 和 q 是素数．*

证明 假定相反，有某个 j 使得 $h_j=p^e>1$．根据习题8.62(ⅱ)，对一切 i 有

$$Z(G/\ker\chi_i)=\{g\in G:|\chi_i(g)|=n_i\}.$$

因 G 是单的，对一切 i，$\ker\chi_i=\{1\}$，从而 $Z(G/\ker\chi_i)=Z(G)=\{1\}$．根据命题 8.152，如果 $(n_i,h_j)=1$，则 $|\chi_i(g_j)|=n_i$ 或 $\chi_i(g_j)=0$．当然对一切 j，$\chi_1(g_j)=1$，其中 χ_1 是平凡特征标．如果 χ_i 不是平凡特征标，则我们刚才已经看到第一种可能性不能出现，从而 $\chi_i(g_j)=0$．另一方面，如果 $(n_i,h_j)\neq 1$，则 $p\mid n_i$(因为 $h_j=p^e$)．于是对每个 $i\neq 1$，$\chi_i(g_j)=0$ 或 $p\mid n_i$．

考虑系8.136(ⅱ)的正交关系：

$$\sum_{i=1}^{r}n_i\,\chi_i(g_j)=0.$$

现在 $n_1=1=\chi_1(g_j)$，而每个其他项或者是 0，或者形如 $p\alpha_i$，其中 α_i 是代数整数．由此，

$$0=1+p\beta,$$

其中 β 是代数整数．这蕴涵有理数 $-1/p$ 是代数整数，因此在 $\mathbb{Z}$ 中，从而得到 $-1/p$ 是整数的矛盾． ■

特征标的另一个早期应用是弗罗贝尼乌斯的定理．我们先讨论双传递置换群．设 G 是有限群和 X 是有限 G-集．回忆如果 $x \in X$，则它的轨道是 $\mathcal{O}(x)=\{gx : g\in G\}$，它的稳定化子是 $G_x = \{g \in G : gx = x\}$．定理 2.98 表明 $|\mathcal{O}(x)||G_x|=|G|$．一个 G-集是传递的，如果它只有一个轨道：如果 x，$y\in X$，则存在 $g\in G$ 使得 $y=gx$；此时，$\mathcal{O}(x)=X$.

如果 X 是 G-集，则存在同态 $\alpha : G\to S_X$，就是 $g\mapsto\alpha_g$，其中 $\alpha_g(x) = gx$．我们称 X 是一个**忠实** G-集，如果 α 是单射；即如果对一切 $x\in X$ 有 $gx=x$，则 $g=1$. 此时，我们把 G 看作 S_X 的子群，其作用是 X 的置换．

凯莱定理（定理 2.87）表明每个群 G 都可看作一个忠实传递 G-集．

637

定义　称一个 G-集 X 是**双传递的**，如果对 $X\times X$ 中 2 元组的每个对 (x_1,x_2) 和 (y_1,y_2)，其中 $x_1 \neq x_2$ 和 $y_1 \neq y_2$，存在 $g \in G$ 使得 $y_1 = gx_1$ 和 $y_2 = gx_2$．⊖

如果存在双传递 G-集，我们常泛称一个群 G 双传递．

注意每个双传递 G-集 X 是传递的：如果 $x\neq y$，则 (x,y) 和 (y,x) 是定义中的 2 元组，从而存在 $g \in G$ 使得 $y = gx$（和 $x = gy$）．

例 8.154　（ⅰ）如果 $n\geqslant 2$，则对称群 S_n 是双传递的；即 $X = \{1,\cdots,n\}$ 是一个双传递 S_X-集．

（ⅱ）如果 $n\geqslant 4$，交错群 A_n 是双传递的．

（ⅲ）设 V 是 $\mathbb{F}_2$ 上的有限维向量空间，并设 $X = V-\{0\}$，则 X 是双传递 $\mathrm{GL}(V)$-集，这是因为 V 中每对不同的非零向量 x_1,x_2 必是线性无关的（见习题 3.69）．因每个线性无关表可以扩张为一个基，因此存在 V 的基 $x_1,x_2,\cdots,x_n$．同样，如果 y_1，y_2 是另一对不同非零向量，则存在基 y_1，$y_2,\cdots,y_n$．但根据习题 3.78，$\mathrm{GL}(V)$ 传递地作用在 V 的一切基的集合上．所以存在 $g \in \mathrm{GL}(V)$ 使得对一切 i 有 $y_i=gx_i$，从而 X 是一个双传递 $\mathrm{GL}(V)$-集．■

命题 8.155　一个 G-集 X 是双传递的当且仅当对每个 $x \in X$，G_x-集 $X-\{x\}$ 是传递的．

证明　设 X 是双传递 G-集．如果 $y,z\in X-\{x\}$，则 (y,x) 和 (z,x) 是 X 中不同元素的 2 元组，因此存在 $g \in G$ 使得 $z = gy$ 和 $x = gx$．后一个等式表明 $g \in G_x$，从而 $X-\{x\}$ 是传递 G_x-集．

为证明逆命题，设 (x_1,x_2) 和 (y_1,y_2) 是 X 的不同元素的 2 元组．我们需要求 $g\in G$ 使得 $y_1 = gx_1$ 和 $y_2 = gx_2$．记 (gx_1,gx_2) 为 $g(x_1,x_2)$．存在 $h \in G_{x_2}$ 使得 $h(x_1,x_2) = (y_1,x_2)$：如果 $x_1 = y_1$，可以取 $h = 1_X$，如果 $x_1\neq y_1$，则用命题假设 $X-\{x_2\}$ 是传递 G_{x_2}-集．同样，存在 $h' \in G_{y_1}$ 使得 $h'(y_1,x_2) = (y_1,y_2)$．所以，$h'h(x_1,x_2) = (y_1,y_2)$，即 X 是双传递 G-集．■

例 8.156　设 k 是域，设 $f(x) \in k[x]$ 没有重根，设 E/k 是分裂域，并设 $G=\mathrm{Gal}(E/k)$ 是 $f(x)$ 的伽罗瓦群．如果 $X = \{\alpha_1,\cdots,\alpha_n\}$ 是 $f(x)$ 一切根的集合，则 X 是一个 G-集（定理 4.3），它是传递的当且仅当 $f(x)$ 是不可约的（命题 4.13）．现在 $f(x)$ 在 $k(\alpha_1)[x]$ 中因式分解为

638

$$f(x) = (x-\alpha_1)f_1(x).$$

读者可以证明 $G_1 = \mathrm{Gal}(E/k(\alpha_1))\leqslant G$ 是稳定化子 G_{α_1}，且 $X-\{\alpha_1\}$ 是 G_1-集．于是命题 8.155 表明 X 是双传递 G-集当且仅当 $f(x)$ 和 $f_1(x)$ 都是不可约的（分别在 $k[x]$ 和 $k(\alpha_1)[x]$ 上）．■

回忆例2.92（ⅱ）：如果 H 是群 G 的子群和 $X=G/H$ 是 H 在 G 中的一切左陪集的族，则 G 由

⊖ 更一般地，我们称一个 G-集 X 为 k-传递的，其中 $1\leqslant k\leqslant|X|$，如果对 $X\times\cdots\times X$ 中的每个有不同坐标的 k 元组对 $(x_1,\cdots,x_k)$ 和 $(y_1,\cdots,y_k)$，存在 $g \in G$ 使得对一切 $i \leqslant k, y_i = gx_i$．可以证明，如果 $k > 5$，则忠实 k-传递群只有对称群和交错群．5 个**马蒂厄（Mathieu）**群是有趣的零星单群，它们也是高传递的：M_{22} 是 3-传递的，M_{11} 和 M_{23} 是 4-传递的，M_{12} 和 M_{24} 是 5-传递的．

$g: aH \mapsto gaH$作用在G/H上．G-集X是传递的，$aH \in G/H$的稳定化子是aHa^{-1}；即$gaH=aH$当且仅当$a^{-1}ga \in H$当且仅当$g \in aHa^{-1}$.

命题 8.157 如果X是双传递G-集，则

$$|G| = n(n-1)|G_{x,y}|,$$

其中$n=|X|$和$G_{x,y}=\{g \in G: gx = x \text{ 和 } gy = y\}$．此外，如果$X$是忠实$G$-集，则$|G_{x,y}|$是$(n-2)!$的因数．

证明 首先，因为X是传递G-集，定理 2.98 给出$|G| = n|G_x|$．现在根据命题 8.155，$X-\{x\}$是传递G_x-集，因$(G_x)_y = G_{x,y}$，从而

$$|G_x| = |X-\{x\}||(G_x)_y| = (n-1)|G_{x,y}|,$$

此时，因$G_{x,y}$是$S_{X-\{x,y\}} \cong S_{n-2}$的子群，从而得到末尾的注记． ■

现在容易给出非双传递群的例子，因为双传递群的阶是有约束的．

定义 一个传递G-集称为**正则的**，如果只有G的幺元固定X的任一元素；即对一切$x \in X$，$G_x=\{1\}$.

例如，凯莱定理表明每个群G同构于S_G的一个正则子群．正则性的概念可以扩张到双传递群上．

定义 一个双传递G-集X称为**强双传递**的，如果只有G的幺元能固定X的两个元素；即对一切不同的对$x,y \in X, G_{x,y}=\{1\}$．

命题 8.158 对忠实双传递G-集X，下面的条件等价，其中$|X|=n$.

（i）X是强双传递的．

（ii）如果(x_1,x_2)和(y_1,y_2)是$X \times X$中的二元组，且$x_1 \neq x_2$和$y_1 \neq y_2$，则存在唯一的 639 $g \in G$使得$y_1 = gx_1$和$y_2 = gy_2$．

（iii）$|G| = n(n-1)$.

（iv）对一切不同的$x,y \in X$，$G_{x,y}=\{1\}$．

（v）对每个$x \in X$，G_x-集$X-\{x\}$是正则的．

证明 所有蕴涵关系都是简单的． ■

例 8.159 （i）S_3和A_4是强双传递群．

（ii）习题 2.46 定义了仿射群$\mathrm{Aff}(1,\mathbb{R})$；它由一切形如$f(x) = ax+b$（其中$a \neq 0$）的函数$f: \mathbb{R} \to \mathbb{R}$在复合运算下组成，而且它同构于由一切形如$\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$的矩阵组成的$\mathrm{GL}(2,\mathbb{R})$的子群．显然，对任意域$k$，我们可以用同样的方法定义$\mathrm{Aff}(1,k)$．特别地，如果$k$是有限域$\mathbb{F}_q$，则仿射群$\mathrm{Aff}(1,\mathbb{F}_q)$是有限的，阶为$q(q-1)$．读者可以验证$\mathbb{F}_q$是强双传递$\mathrm{Aff}(1,\mathbb{F}_q)$-集． ■

记号 如果G是群，则$G^\# = \{g \in G: g \neq 1\}$.

根据凯莱定理，每个群都是正则的．我们现在考虑对每个$g \in G^\#$最多有一个固定点的传递群G. 在每个$g \in G^\#$都没有固定点的情形，我们说G的作用是**无固定点**的．汤普森证明：如果有限群H有一个无固定点的素数阶自同态α（即群$G=\langle \alpha \rangle$在$H^\#$上的作用无固定点），则H是幂零的（见 Robinson 所著的《A Course in the Theory of Groups》，306～307 页）．于是，我们考虑存在 1 个固定点的某个$g \in G^\#$的作用；即G的作用不是正则的．

定义 一个有限群G称为**弗罗贝尼乌斯群**，如果存在传递G-集满足

（i）每个$g \in G^\#$最多有一个固定点；

（ⅱ）存在某个 $g\in G^{\#}$ 恰有一个固定点．

如果 $x\in X$，我们称 G_x 为 G 的**弗罗贝尼乌斯补**．

注意条件（ⅰ）蕴涵定义中的 G-集 X 必是忠实的．我们重新叙述这两个条件：（ⅰ）每个 $g\in G^{\#}$ 最多有一个固定点是说 $G_{x,y}=\{1\}$；（ⅱ）存在某个 $g\in G^{\#}$ 恰有一个固定点是说 $G_x\neq\{1\}$．

例 8.160　（ⅰ）对称群 S_3 是弗罗贝尼乌斯群：$X=\{1,2,3\}$ 是忠实传递 S_3-集；没有 $\alpha\in(S_3)^{\#}$ 固定两个元素，每个对换 $(i\,j)$ 固定一个元素．循环子群 $\langle(i\,j)\rangle$ 是弗罗贝尼乌斯补（因此弗罗贝尼乌斯补不必是唯一的）．置换 $\beta\in S_3$ 没有固定点当且仅当 β 是 3-轮换．我们准备证明在弗罗贝尼乌斯群中，1 和没有固定点的那些元素一起构成正规子群．　640

（ⅱ）可以推广（ⅰ）中 S_3 的例子．设 X 是 G-集，它至少有三个元素，而且是一个强双传递 G-集．则 X 是传递的，$G_{x,y}=\{1\}$，且 $G_x\neq\{1\}$（因为对不同的 $x,y,z\in X$，存在 $g\in G$ 使得 $x=gx$ 和 $z=gy$）．所以每个强双传递群 G 是弗罗贝尼乌斯群．■

命题 8.161　有限群 G 是弗罗贝尼乌斯群当且仅当它包含一个非平凡真子群 H，且对一切 $g\notin H$，$H\cap gHg^{-1}=\{1\}$．

证明　设 X 是弗罗贝尼乌斯群定义中的 G-集．选取 $x\in X$，并定义 $H=G_x$．现在因为传递性不允许对一切 $g\in G$ 有 $gx=x$，所以 H 是 G 的真子群．为证明 H 是非平凡的，选取有一个固定点的 $g\in G^{\#}$，比如 $gy=y$．如果 $y=x$，则 $g\in G_x=H$．如果 $y\neq x$，则传递性给出 $h\in G$ 使得 $hy=x$，习题 2.99 给出 $H=G_x=hG_yh^{-1}\neq\{1\}$．如果 $g\notin H$，则 $gx\neq x$．现在 $g(G_x)g^{-1}=G_{gx}$．因此，如果 $h\in H\cap gHg^{-1}=G_x\cap G_{gx}$，则 h 固定 x 和 gx；即 $h\in G_{x,y}=\{1\}$．

关于逆命题，取 X 为 H 在 G 中的一切左陪集的 G-集 G/H，其中对一切 $g\in G$，$g: aH\mapsto gaH$．我们早先注释过 X 是一个传递 G-集，且 $aH\in G/H$ 的稳定化子是 G 的子群 aHa^{-1}．因 $H\neq\{1\}$，可知 $G_{aH}\neq\{1\}$．最后，如果 $aH\neq bH$，则因 $a^{-1}b\notin H$，有

$$G_{aH,bH}=G_{aH}\cap G_{bH}=aHa^{-1}\cap bHb^{-1}=a(H\cap a^{-1}bHb^{-1}a)a^{-1}=\{1\},$$

所以 G 是弗罗贝尼乌斯群．■

上面这个命题的重要性在于它把弗罗贝尼乌斯群的定义从 G-集的语言翻译为抽象群的语言．

定义　如果 X 是 G-集，定义它的**弗罗贝尼乌斯核**为子集

$$N=\{1\}\cup\{g\in G: g\text{ 没有固定点}\}.$$

当 X 传递时，可以用稳定化子 G_x 来描述 N．如果 $a\notin N^{\#}$，则存在某个 $y\in X$ 使得 $ay=y$．因 G 的作用是传递的，存在 $g\in G$ 使得 $gx=y$，且 $a\in G_y=gG_xg^{-1}$．因此 $a\in\bigcup_{g\in G}gG_xg^{-1}$．关于反包含，如果 $a\in\bigcup_{g\in G}gG_xg^{-1}$，则有某个 $g\in G$ 使得 $a\in gG_xg^{-1}=G_{gx}$，从而 a 有一个固定点；即 $a\notin N$．我们已经证明了

$$N=\{1\}\cup\Big(G-\Big(\bigcup_{g\in G}gG_xg^{-1}\Big)\Big).$$

习题 5.32 表明，如果 G_x 是 G 的真子群，则 $G\neq\bigcup_{g\in G}gG_xg^{-1}$，从而此时 $N\neq\{1\}$．　641

命题 8.162　如果 G 是有弗罗贝尼乌斯补 H 和弗罗贝尼乌斯核 N 的弗罗贝尼乌斯群，则 $|N|=[G:H]$．

证明　根据命题 8.161，有不相交并

$$G = \{1\} \cup \left(\bigcup_{g\in G} gH^{\#}g^{-1}\right) \cup N^{\#}.$$

注意 $N_G(H) = H$：如果 $g \notin H$，则 $H \cap gHg^{-1} = \{1\}$，从而 $gHg^{-1} \neq H$. 因此，H 的共轭的个数是 $[G : N_G(H)] = [G : H]$（命题 2.101）. 所以，$\left|\bigcup_{g\in G} gH^{\#}g^{-1}\right| = [G : H](|H|-1)$，因此

$$|N| = |N^{\#}| + 1 = |G| - ([G : H](|H|-1)) = [G : H].$$ ■

弗罗贝尼乌斯核可以不是 G 的子群．容易验证，如果 $g \in N$，则 $g^{-1} \in N$，且对每个 $a \in G, aga^{-1} \in N$；困难的是证明 N 在乘法下封闭．例如，如果 $V = k^n$ 是域 k 上一切 $n \times 1$ 列向量的向量空间，则 $V^{\#}$，即 V 中非零向量的集合是忠实传递 $\mathrm{GL}(V)$ -集．现在 $A \in \mathrm{GL}(V)$ 有一个固定点当且仅当存在某个 $v \in V^{\#}$ 使得 $Av = v$；即 A 有一个固定点当且仅当 1 是 A 的特征值．于是，弗罗贝尼乌斯核由单位矩阵和一切不以 1 为特征值的线性变换组成．设 $|k| \geq 4$，并设 α 是 k 的非零元素满足 $\alpha^2 \neq 1$，则 $A = \begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix}$和 $B = \begin{bmatrix} \alpha^{-1} & 0 \\ 0 & \alpha \end{bmatrix}$ 在 N 中，但它们的积 $AB = \begin{bmatrix} 1 & 0 \\ 0 & \alpha^2 \end{bmatrix}$ 不在 N 中．然而，如果 G 是弗罗贝尼乌斯群，则 N 是子群；这个事实的已知证明只有运用特征标才能完成．

我们已经注明，如果 ψ 是群 G 的子群 H 上的特征标，则限制 $(\psi\!\uparrow^G)_H$ 未必等于ψ. 下一个证明表明一个弗罗贝尼乌斯补的不可约特征标能够扩张为 G 的不可约特征标．

引理 8.163 设 G 是有弗罗贝尼乌斯补 H 和弗罗贝尼乌斯核 N 的弗罗贝尼乌斯群．对 H 上的每个不是平凡特征标ψ_1 的不可约特征标ψ，定义广义特征标

$$\varphi = \psi - d\psi_1,$$

其中 $d = \psi(1)$. 则 $\psi^* = \varphi\!\uparrow^G + d\chi_1$ 是 G 上的不可约特征标，且 $\psi^*_H = \psi$；即对一切 $h \in H, \psi^*(h) = \psi(h)$.

证明 首先注意 $\varphi(1) = 0$. 我们断言诱导广义特征标 $\varphi\!\uparrow^G$满足等式

$$(\varphi\!\uparrow^G)_H = \varphi.$$

如果 $t_1 = 1, \cdots, t_n$ 是 H 在 G 中的陪集代表系，则对 $g \in G, \varphi\!\uparrow^G(g)$ 的矩阵的对角线上是块 $\dot{B}(t_i^{-1}gt_i)$，其中，如果 $t_i^{-1}ht_i \notin H$，则 $\dot{B}(t_i^{-1}gt_i) = 0$（这正是定理 8.142 的矩阵形式）. 如果 $h \in H$，则对一切 $i \neq 1, t_i^{-1}ht_i \notin H$, 从而 $\dot{B}(t_i^{-1}ht_i) = 0$. 所以对角线上只有一个非零块，且

642

$$\mathrm{tr}(\varphi\!\uparrow^G(h)) = \mathrm{tr}(B(h));$$

即

$$\varphi\!\uparrow^G(h) = \varphi(h).$$

我们已经看到 $\varphi\!\uparrow^G$ 是 G 上的广义特征标满足 $(\varphi\!\uparrow^G)_H = \varphi$. 根据弗罗贝尼乌斯互反性（定理 8.145），

$$(\varphi\!\uparrow^G, \varphi\!\uparrow^G)_G = (\varphi, (\varphi\!\uparrow^G)_H)_H = (\varphi, \varphi)_H.$$

但 $\varphi = \psi - d\psi_1$，因此ψ和ψ_1 的正交性给出

$$(\varphi, \varphi)_H = 1 + d^2.$$

同样，

$$(\varphi\!\uparrow^G, \chi_1)_G = (\varphi, \psi_1)_H = -d,$$

其中 χ_1 是 G 上的平凡特征标．定义

$$\psi^* = \varphi\uparrow^G + d\chi_1.$$

现在ψ^*是G上的广义特征标，且

$$(\psi^*, \psi^*)_G = (\varphi\uparrow^G, \varphi\uparrow^G)_G + 2d(\varphi\uparrow^G, \chi_1)_G + d^2$$
$$= 1 + d^2 - 2d^2 + d^2 = 1.$$

我们有

$$(\psi^*)_H = (\varphi\uparrow^G)_H + d(\chi_1)_H = \varphi + d\psi_1 = (\psi - d\psi_1) + d\psi_1 = \psi.$$

因$\psi^*(1) = \psi(1) > 0$，系 8.130 说ψ^*是G上的不可约特征标． ■

定理 8.164（弗罗贝尼乌斯） *设G是有弗罗贝尼乌斯补H和弗罗贝尼乌斯核N的弗罗贝尼乌斯群，则N是G的正规子群，$N \cap H = \{1\}$，且$NH = G$.*

注 *群G有子群Q和正规子群K满足$K \cap Q = \{1\}$和$KQ = G$叫做半直积．第 10 章中要讨论这种群．*

证明 对H上的每个不是平凡特征标ψ_1的不可约特征标ψ，定义广义特征标$\varphi = \psi - d\psi_1$，其中$d = \psi(1)$．根据引理，$\psi^* = \varphi\uparrow^G + d\chi_1$是$G$上的不可约特征标．定义

$$N^* = \bigcap_{\psi \neq \psi_1} \ker \psi^*.$$

当然，N^*是G的正规子群．

643

根据引理 8.163，对一切$h \in H$，$\psi^*(h) = \psi(h)$；特别地，如果$h = 1$，有

$$\psi^*(1) = \psi(1) = d. \tag{5}$$

如果$g \in N^\#$，则对一切$a \in G$，有$g \notin aHa^{-1}$（因为g没有固定点），从而$\dot{\varphi}(aga^{-1}) = 0$．现在诱导特征标公式，即定理 8.142 给出$\varphi\uparrow^G(g) = 0$．因此，如果$g \in N^\#$，则等式（5）给出

$$\psi^*(g) = \varphi\uparrow^G(g) + d\chi_1(g) = d.$$

由此推出，如果$g \in N$，则

$$\psi^*(g) = d = \psi^*(1);$$

即$g \in \ker \psi^*$．所以

$$N \subseteq N^*.$$

反包含来自计算论证．

设$h \in H \cap N^*$．因$h \in H$，引理 8.163 给出$\psi^*(h) = \psi(h)$．另一方面，因$h \in N^*$，有$\psi^*(h) = \psi^*(1) = d$．所以$\psi(h) = \psi^*(h) = d = \psi(1)$，从而对$H$上的每个不可约特征标$\psi$有$h \in \ker \psi$．考虑由$H$上的正则表示$\rho$提供的正则特征标：$\chi_\rho = \sum_i n_i \psi_i$．现在$\chi_\rho(h) = \sum_i n_i \psi_i(h) \neq 0$，因此例 8.125（ⅱ）给出$h = 1$．于是，

$$H \cap N^* = \{1\}.$$

其次，根据命题 8.162，$|G| = |H|[G:H] = |H||N|$．注意，因为$N^* \lhd G$，所以HN^*是G的子群．现在根据第二同构定理，$|HN^*||H \cap N^*| = |H||N^*|$；因$H \cap N^* = \{1\}$，有$|H||N| = |G| \geqslant |HN^*| = |H||N^*|$．因此，$|N| \geqslant |N^*|$．但因$N \subseteq N^*$，有$|N| \leqslant |N^*|$，从而$N = N^*$．所以，$N \lhd G, H \cap N = \{1\}, HN = G$． ■

关于弗罗贝尼乌斯群的结构可说的还有很多．弗罗贝尼乌斯补的每个西罗子群是循环群或

广义四元数群（见 Huppert 所著的《Endliche Gruppen I》502 页），关于无固定点自同态的汤普森定理有一个推论说每个弗罗贝尼乌斯核是幂零的；即 N 是它的西罗子群的直积．读者可参考 Curtis-Reiner 所著的《Representation Theory of Finite Groups and Associative Algebras》242～246 页，或 Feit 所著的《Characters of Finite Groups》133～139 页．

644

习题

8.68 证明例8.159(ⅱ)中的仿射群 $\text{Aff}(1,\mathbb{F}_q)$ 是强双传递的．

8.69 如果 $H\leqslant G$，且左陪集的族 G/H 经由陪集上的表示成为一个 G-集，证明 G/H 是忠实 G-集当且仅当 $\bigcap_{a\in G} aHa^{-1}=\{1\}$．举出一个 G/H 不是忠实 G-集的例子．

8.70 证明 $SL(2,\mathbb{F}_5)$ 的每个西罗子群是循环群或四元数群．

8.71 群 G 的一个子集 A 叫做 **T. I. 集（或平凡交集）**，如果 $A\subseteq N_G(A)$ 且对一切 $g\notin N_G(A)$ 有 $A\cap gAg^{-1}\subseteq\{1\}$．

(ⅰ) 证明弗罗贝尼乌斯群 G 的弗罗贝尼乌斯补 H 是一个 T. I. 集．

(ⅱ) 设 A 是有限群 G 中的一个 T. I. 集，并设 $N=N_G(A)$．如果 α 是把 $N-A$ 变为 0 的类函数，β 是把 $(\bigcup_{g\in G}(A^g\cap N))-A$ 变为 0 的 N 上的类函数，证明对一切 $g\in N^{\#}$，有 $\alpha^{G}(g)=\alpha(g)$ 和 $\beta^{G}(g)=\beta(g)$．

提示：见引理 8.164 和定理 8.163 的证明．

(ⅲ) 如果 $\alpha(1)=0$，证明 $(\alpha,\beta)_N=(\alpha^G,\beta^G)_G$.

(ⅳ) 设 H 是有限群 G 的一个自正规化子群；即 $H=N_G(H)$．如果 H 是 T. I. 集，证明存在 G 的正规子群 K 使得 $K\cap H=\{1\}$ 和 $KH=G$.

提示：见 Feit 所著的《Characters of Finite Groups》124 页．

8.72 证明存在 n 阶非阿贝尔单群，其中 $60<n\leqslant 100$.

提示：根据伯恩赛德定理，在 n 的给定的区间中，只有 66，70，78，84 和 90 可能作为基数，而 90 被习题5.29(ⅱ)排除．

8.73 证明存在 n 阶非阿贝尔单群，其中 $101\leqslant n\leqslant 168$. 我们说明 $PSL(2,\mathbb{F}_7)$ 是 168 阶单群，如果不计同构，它是唯一的这样的群．由命题 5.41、系 5.68 和习题 8.72 可知阶严格小于 168 的非阿贝尔单群只有 A_5.

提示：根据伯恩赛德定理，在 n 的给定区间中，可能作为基数的只有 102，105，110，120，126，130，132，138，140，150，154，156 和 165. 运用习题 2.98、习题 5.30 和习题 5.31.

645

第9章　高等线性代数

本章先研究PID上的模，涉及它们的投射、内射和平坦模的刻画．然而，我们强调的是有限生成模，因为有限阿贝尔群基本定理的推广在应用到 $k[x]$-模时，产生矩阵的有理典范型和若尔当典范型．也要讨论史密斯正规型，因为它可以用来计算矩阵的不变量．然后考虑向量空间上的双线性型和二次型，它们导出辛群和正交群．下一步是多重线性代数，接着是向张量代数、外代数和行列式．最后介绍李代数，它可以看作处理线性变换族的一种方法，而原先只是进行个别的讨论．

9.1　PID上的模

现在把有限阿贝尔群的结构定理推广到PID上的模．正如我们说过的，这个推广不仅是为了它自身的缘故，更因为模的版本产生矩阵的典范型．我们将看到不但定理推广了，而且定理的证明也推广了．

定义　设 M 是 R-模．如果 $m\in M$，则它的**阶理想**（或**零化子**）是指

$$\operatorname{ann}(m)=\{r\in R : rm=0\}.$$

我们说 m **有有限阶**（或是一个挠[⊖]元），如果 $\operatorname{ann}(m)\neq\{0\}$；否则 m **有无限阶**．

当一个交换环 R 看作它自身上的模时，它的幺元 1 有无限阶，这是因为 $\operatorname{ann}(1)=\{0\}$．　[646]

阶理想推广了群论中元素的阶的概念．回忆如果 G 是加法阿贝尔群，则一个元素 $g\in G$ 有有限阶，如果有某个正整数 n 使得 $ng=0$，而 g 的阶为 d，如果 d 是最小的正整数使得 $dg=0$．另一方面，$\operatorname{ann}(g)$ 是 $\mathbb{Z}$ 中的理想，和 $\mathbb{Z}$ 中的任意非零理想一样，它由其中的最小正整数生成．于是阶理想 $\operatorname{ann}(g)=(d)$，它是由 g 的阶 d 生成的主理想．在命题7.12中，我们证明如果 $M=\langle m\rangle$ 是循环 R-模,其中 R 是任意交换环，则 $M\cong R/I$．在这个推论中，理想 I 是 $\ker\varphi$，其中 $\varphi: R\to M$ 是映射 $r\mapsto rm$，从而 $I=\operatorname{ann}(m)$，且

$$\langle m\rangle\cong R/\operatorname{ann}(m).$$

定义　如果 M 是 R-模,其中 R 是整环，则它的**挠子模**[⊜] tM 定义为

$$tM=\{m\in M : m\text{ 有有限阶}\}.$$

命题9.1　如果 R 是整环和 M 是 R-模,则 tM 是 M 的子模．

证明　如果 $m,m'\in tm$，则存在非零元素 $r,r'\in R$ 使得 $rm=0$ 和 $r'm'=0$. 显然，$rr'(m+m')=0$．因 R 是整环，$rr'\neq 0$，从而 $\operatorname{ann}(m+m')\neq\{0\}$；所以 $m+m'\in tM$．

如果 $s\in R$，则因 $rsm=0$，从而 $r\in\operatorname{ann}(sm)$，所以 $sm\in tM$．　■

如果 R 不是整环，该命题不成立．例如，设 $R=\mathbb{I}_6$．在 $M=\mathbb{I}_6$ 中，因为 $[2]\in\operatorname{ann}([3])$ 和 $[3]\in\operatorname{ann}([4])$，所以 $[3]$ 和 $[4]$ 都有有限阶．另一方面，$[3]+[4]=[1]$，因 $\operatorname{ann}([1])=\{0\}$，所以 $[1]$ 在 M 中有无限阶．

⊖　267页上给出了torsion（挠）的词源．

⊜　挠子模有一个推广，叫做奇异子模，它是对未必交换的环上的左 R-模定义的．见Dauns所著的《Modules and Rings》，231～238页．

本节的剩下部分中，R 都是整环（其实早就应限制了）.

定义 假定 R 是整环和 M 是 R-模，则称 M 是挠的，如果 $tM = M$，而称 M 是无挠的，如果 $tM = \{0\}$.

命题 9.2 设 M 和 M' 都是 R-模，其中 R 是整环.

（i）M/tM 是无挠的.

（ii）如果 $M \cong M'$，则 $tM \cong tM'$ 和 $M/tM \cong M'/tM'$.

证明 （i）假定在 M/tM 中 $m + tM \neq 0$；即 m 有无限阶. 如果 $m + tM$ 有有限阶，则存在某个 $r \in R$ 且 $r \neq 0$ 满足 $0 = r(m + tM) = rm + tM$；即 $rm \in tM$. 于是存在 $s \in R$ 且 $s \neq 0$ 使得 $0 = s(rm) = (sr)m$. 但因 R 是整环，所以 $sr \neq 0$，从而 $\operatorname{ann}(m) \neq \{0\}$；这与 m 有无限阶矛盾.

647

（ii）如果 $\varphi: M \to M'$ 是同构，则因对 $rm = 0$ 且 $r \neq 0$ 有 $r\varphi(m) = \varphi(rm) = 0$（这对任意$R$-同态都成立），所以 $\varphi(tM) \subseteq tM'$；因此 $\varphi \mid tM: tM \to tM'$ 是同构（逆为 $\varphi^{-1} \mid tM'$）. 关于第二个陈述，易知定义为 $\overline{\varphi}: m + tM \mapsto \varphi(m) + tM'$ 的映射 $\overline{\varphi}: M/tM \to M'/tM'$ 是同构. ■

这里是命题 9.2 的一个奇特的证明. 存在函子 $t: {}_R\mathbf{Mod} \to {}_R\mathbf{Mod}$，在模上定义为 $M \mapsto tM$，在态射上定义为 $\psi \mapsto \psi \mid tM$. 由每个函子保持等价的事实得 $tM \cong tM'$.

非诺特交换环 R 本来的定义是有一个理想不是有限生成的. 现在把 R 看作它自身上的模则是有限生成的；事实上，它是循环的（生成元为 1）. 于是，有可能一个有限生成模的子模未必是有限生成的. 当 R 是 PID 时，不会发生这种情形；事实上，我们在命题 7.23（ii）中已经证明，如果 R 是 PID，则有限生成模 R-的每个子模 S 是有限生成的；其实，如果 M 能由 n 个元素生成，则 S 能由 n 个或少于 n 个元素生成.

定理 9.3 如果 R 是 PID，则每个有限生成无挠 R-模 M 是自由模.

证明 我们对 n 用归纳法证明这个定理，其中 $M = \langle v_1, \cdots, v_n \rangle$.

如果 $n = 1$，则 M 是循环模；因此 $M = \langle v_1 \rangle \cong R/\operatorname{ann}(v_1)$. 因 M 是无挠的，$\operatorname{ann}(v_1) = \{0\}$，从而 $M \cong R$，因此 M 是自由的.

关于归纳步，设 $M = \langle v_1, \cdots, v_{n+1} \rangle$，并定义

$$S = \{m \in M: \text{存在 } r \in R, r \neq 0 \text{ 使得 } rm \in \langle v_{n+1} \rangle\};$$

容易验证 S 是 M 的子模. 现在 M/S 是无挠的：如果 $x \in M, x \notin S, r(x + S) = 0$，则 $rx \in S$；因此存在 $r' \in R$ 满足 $r' \neq 0$ 和 $rr'x \in \langle v_{n+1} \rangle$. 因 $rr' \neq 0$，有 $x \in S$，这是一个矛盾. 显然，M/S 能由 n 个元素生成，就是 $v_1 + S, \cdots, v_n + S$，从而根据归纳假设，M/S 是自由的. 因自由模是投射的，所以命题 7.54 给出

$$M \cong S \oplus (M/S).$$

于是只要证明 $S \cong R$，证明就得以完成.

如果 $x \in S$，则存在某个非零 $r \in R$ 使得 $rx \in \langle v_{n+1} \rangle$；即存在 $a \in R$ 使得 $rx = av_{n+1}$. 定义 $\varphi: S \to Q = \operatorname{Frac}(R)$ 为 $\varphi: x \mapsto a/r$，其中 $\operatorname{Frac}(R)$ 是 R 的分式域. 经简单计算（留给读者）可知 φ 是（合理定义的）单射 R-映射. 如果 $D = \operatorname{im}\varphi$，则 D 是 Q 的有限生成子模. 因为 S 是 M 的直和项，因此是 M 的象，所以 $D \cong S$ 是有限生成的.

如果能够证明 Q 的每个有限生成子模 D 都是循环的，就可完成证明. 现在

$$D = \langle b_1/c_1, \cdots, b_m/c_m \rangle,$$

其中 $b_i, c_i \in R$. 令 $c = \prod_i c_i$，并定义 $f: D \to R$ 为对一切 $d \in D$，$f: d \mapsto cd$（因为乘 c 清除了一切分母，所以 f 的值在 R 中）. 因 D 是无挠的，f 是单射 R-映射，从而 D 同构于 R 的一个子模；即 D 同构于 R 的一个理想. 因 R 是 PID，R 中的每个非零理想同构于 R；因此 $S \cong \operatorname{im}\varphi = D \cong R$. ■ [648]

系 9.4 如果 R 是 PID，则有限生成自由 R-模 F 的每个子模 S 是自由的，且 $\operatorname{rank}(S) \leqslant \operatorname{rank}(F)$. 特别地，每个有限生成投射 R-模 P 是自由的.

证明 根据命题7.23(ⅱ)，子模 S 能够由 n 个或少于 n 个元素生成，其中 $n = \operatorname{rank}(F)$. 现在 F 是无挠的，因此 S 是无挠的. 运用定理 9.3 得到 S 是自由的.

第二个陈述来自定理 7.56：投射模作为自由模的直和项的特性. 因 P 是有限生成的，存在有限生成自由模 F 和满射 $q: F \to P$；因 P 是投射的，存在映射 $j: P \to F$ 使得 $qj = 1_P$. 于是 j 局限于 P 和 F 的一个子模的同构，根据第一部分的证明，这个子模是自由的. ■

注 没有有限性的假设，系中的两个陈述也真，我们将很快证明它们.

系 9.5 (ⅰ) 如果 R 是 PID，则每个有限生成 R-模 M 是一个直和

$$M = tM \oplus F,$$

其中 F 是一个有限生成自由 R-模.

(ⅱ) 如果 M 和 M' 都是有限生成 R-模，其中 R 是 PID，则 $M \cong M'$ 当且仅当 $tM \cong tM'$ 和 $\operatorname{rank}(M/tM) = \operatorname{rank}(M'/tM')$.

证明 (ⅰ) 因为 M 是有限生成的，所以商模 M/tM 是有限生成的，根据命题 9.2(ⅰ)，M/tM 是无挠的. 所以根据定理 9.3，M/tM 是自由的，因此 M/tM 是投射的. 最后，根据系 7.55，$M \cong tM \oplus (M/tM)$.

(ⅱ) 根据命题9.2(ⅱ)，如果 $M \cong M'$，则 $tM \cong tM'$ 和 $M/tM \cong M'/tM'$. 因 M/tM 是有限生成无挠的，所以它是自由模，M'/tM' 也是如此，如果它们有相同的秩，则它们是同构的.

反之，因 $M \cong tM \oplus (M/tM)$ 和 $M' \cong tM' \oplus (M'/tM')$，命题 7.30 把每个直和项上的同构组合成同构 $M \to M'$. ■

注 这个系需要有限生成的假设. 存在阿贝尔群 G，它的挠子群 tG 不是 G 的直和项［见习题9.1(ⅲ)］.

现在我们可以刻画 PID 上的平坦模. [649]

系 9.6 如果 R 是 PID，则 R-模是平坦的当且仅当它是无挠的.

证明 根据定理 9.3，每个有限生成无挠 R-模都是自由的，从而根据引理 8.98，它是平坦的. 根据引理 8.97，M 是平坦的.

反之，如果 M 不是无挠的，则它包含一个有限阶的非零元素 m，比如阶为 (r). 如果 $i: R \to \operatorname{Frac}(R)$ 是包含映射，则 $m \otimes 1 \in \ker(1_M \otimes i)$，这是因为在 $M \otimes_R \operatorname{Frac}(R)$ 中，有

$$m \otimes 1 = m \otimes \frac{r}{r} = rm \otimes \frac{1}{r} = 0.$$

另一方面，根据命题 8.86，映射 $m \otimes 1 \mapsto m$ 是同构 $M \otimes_R R \to M$，从而在 $M \otimes_R R$ 中，$m \otimes 1 \neq 0$. 所以 M 不是平坦的. ■

在继续进行有限生成模的详尽讨论之前，我们暂且证明一个重要结果：系 9.4 的推广，其中不再假设自由模 F 是有限生成的. 我们先给出有限生成情形下的第二个证明，然后再推广.

命题 9.7 如果 R 是 PID，则有限生成自由 R-模 F 的每个子模 H 是自由的，且 $\operatorname{rank}(H) \leqslant \operatorname{rank}(F)$.

证明 对 $n=\text{rank}(F)$ 用归纳法证明．如果 $n=1$，则 $F\cong R$．于是 H 同构于 R 中的一个理想；但一切理想都是主理想，因此同构于 $\{0\}$ 或 R. 所以 H 是秩 $\leqslant 1$ 的自由模．

现在我们证明归纳步．如果 $\{x_1,\cdots,x_{n+1}\}$ 是 F 的基，定义 $F'=\langle x_1,\cdots,x_n\rangle$，并设 $H'=H\cap F'$．根据归纳假设，H' 是秩 $\leqslant n$ 的自由模．现在

$$H/H'=H/(H\cap F')\cong(H+F')/F'\subseteq F/F'\cong R.$$

根据基础步，或者 $H/H'=\{0\}$，或者 $H/H'\cong R$．在第一种情形中，$H=H'$，证明完成．在第二种情形中，系 7.55 给出对某个 $h\in H$ 有 $H=H'\oplus\langle h\rangle$，其中 $\langle h\rangle\cong R$，因此 H 是自由阿贝尔模，而且秩 $\leqslant n+1$． ■

我们现在去掉有限性的假设．

定理 9.8 *如果 R 是 PID，则自由 R-模 F 的每个子模 H 是自由的，且 $\text{rank}(H)\leqslant\text{rank}(F)$．特别地，每个投射 R-模都是自由的．*

证明 我们要用到选择公理和佐恩引理的等价陈述（见附录），即每个集合都可以是良序的．特别地，可以假定 F 的基 $\{x_k:k\in K\}$ 有良序指标集 K.

对每个 $k\in K$，定义

$$F'_k=\langle x_j:j\prec k\rangle \text{ 和 } F_k=\langle x_j:j\preceq k\rangle=F'_k\oplus\langle x_k\rangle;$$

注意 $F=\bigcup_k F_k$．定义

650

$$H'_k=H\cap F'_k \text{和 } H_k=H\cap F_k.$$

现在 $H'_k=H\cap F'_k=H_k\cap F'_k$，从而

$$\begin{aligned}H_k/H'_k&=H_k/(H_k\cap F'_k)\\&\cong(H_k+F'_k)/F'_k\subseteq F_k/F'_k\cong R.\end{aligned}$$

根据系 7.55，或者 $H_k=H'_k$，或者 $H_k=H'_k\oplus\langle h_k\rangle$，其中 $h_k\in H_k\subseteq H$ 且 $\langle h_k\rangle\cong R$．我们断言 H 是以一切 h_k 的集合为基的自由 R-模．这就导出 $\text{rank}(H)\leqslant\text{rank}(F)$．

因 $F=\bigcup F_k$，每个 $f\in F$ 在某个 F_k 中；因 K 是良序集，存在最小指标 $k\in K$ 使得 $f\in F_k$，记这个最小指标为 $\mu(f)$，特别地，如果 $h\in H$，则

$$\mu(h)=\text{最小指标 } k \text{ 使得 } h\in F_k.$$

注意，如果 $h\in H'_k\subseteq F'_k$，则 $\mu(h)\prec k$．设 H^* 是由一切 h_k 生成的 H 的子模．

假设 H^* 是 H 的真子模．令 j 是

$$\{\mu(h):h\in H \text{ 和 } h\notin H^*\}$$

中的最小指标，并选取 $h'\in H$ 为有指标 j 的元素；即 $h'\notin H^*$ 和 $\mu(h')=j$．现在因为 $\mu(h')=j$ 有 $h'\in H\cap F_j$，从而

$$h'=a+rh_j,\text{其中 } a\in H'_j \text{和 } r\in R.$$

于是 $a=h'-rh_j\in H'_j$ 和 $a\notin H^*$，否则 $h'\in H^*$（因为 $h_j\in H^*$）．因 $\mu(a)\prec j$，这和 j 是在 H 中而不在 H^* 的元素的最小指标矛盾．由此推出 $H^*=H$；即每个 $h\in H$ 都是各个 h_k 的线性组合．

剩下的要证明任一 $h\in H$ 的作为各个 h_k 的线性组合的表达式唯一．把这样的两个表达式相减，从而只需证明如果

$$0=r_1h_{k_1}+r_2h_{k_2}+\cdots+r_nh_{k_n},$$

则一切系数 $r_i=0$．把上式中的项排成 $k_1\prec k_2\prec\cdots\prec k_n$．如果 $r_n\neq0$，则 $r_nh_{k_n}\in\langle h_{k_n}\rangle\cap H'_{k_n}=$

$\{0\}$，产生矛盾．所以一切 $r_i = 0$，从而 H 是以 $\{h_k : k \in K\}$ 为基的自由模． ■

我们回到有限生成模的讨论．根据命题9.2(ⅱ)，当 R 是 PID 时，有限生成 R-模的分类问题简化为有限生成挠模的分类问题．我们立即说明这些模就是有限阿贝尔群的推广．

651

命题 9.9 一个阿贝尔群是有限的当且仅当它是有限生成挠$\mathbb{Z}$-模．

证明 如果 G 是有限的，它显然是有限生成的；此外，拉格朗日定理说 G 是挠的．

反之，假定 $G = \langle x_1, \cdots, x_n \rangle$，并存在非零整数 d_i 使得对一切 i，$d_i x_i = 0$．由此，每个 $g \in G$ 可以写成

$$g = m_1 x_1 + \cdots + m_n x_n,$$

其中对一切 i，$0 \leqslant m_i < d_i$．所以，$|G| \leqslant \prod_i d_i$，因此 G 是有限的． ■

定义 设 R 是 PID 和 M 是 R-模．如果 $P = (p)$ 是 R 中的非零素理想，则 M 称为(p)-**准素的**，如果对每个 $m \in M$，存在 $n \geqslant 1$ 使得 $p^n m = 0$．

如果 M 是任意 R-模，则它的 (p) -**准素分量**是指

$$M_P = \{m \in M : 有某个\ n \geqslant 1\ 使得\ p^n m = 0\}.$$

如果不想特别指定素理想 P，则可以称一个模是准素的（代替 P-准素）．显然准素分量是子模．

本节接下来的所有定理先对阿贝尔群证明，然后推广到 PID 上的模．从阿贝尔群到模的翻译是简单的，但为了更清楚地了解这个翻译，我们修改第 5 章中对阿贝尔群的准素分解的证明，从而把它推广到 PID 上的模的准素分解．为了读者的方便，我们去掉有限性的假设重做这个证明．

定理 9.10（准素分解） （ⅰ）每个挠阿贝尔群 G 是它的 p-准素分量的直和：

$$G = \sum_p G_p.$$

（ⅱ）每个挠 R-模 M（其中 R 是 PID）是它的 P-准素分量的直和：

$$M = \sum_P M_P.$$

证明 （ⅰ）设 $x \in G$ 非零，并设它的阶为 d．根据算术基本定理，存在不同的素数 $p_1, \cdots, p_n$ 和正指数 $e_1, \cdots, e_n$ 使得

$$d = p_1^{e_1} \cdots p_n^{e_n}.$$

定义 $r_i = d/p_i^{e_i}$，从而 $p_i^{e_i} r_i = d$．由此，对每个 i，$r_i x \in G_{p_i}$．但 $r_1, \cdots, r_n$ 的 gcd 是 1，从而存在整数 $s_1, \cdots, s_n$ 使得 $1 = \sum_i s_i r_i$．所以，

$$x = \sum_i s_i r_i x \in \left\langle \bigcup_p G_p \right\rangle.$$

652

对每个素数 p，记 $H_p = \left\langle \bigcup_{q \neq p} G_q \right\rangle$．根据习题 7.79，只要证明如果

$$x \in G_p \cap H_p,$$

则 $x=0$．因 $x \in G_p$，有某个 $\ell \geqslant 0$ 使得 $p^\ell x = 0$；因 $x \in H_p$，有 $ux = 0$，其中 $u = q_1^{f_1} \cdots q_n^{f_n}$，$q_i \neq p$，且对一切 i，$f_i \geqslant 1$．但 p^ℓ 和 u 互素，因此存在整数 s 和 t 使得 $1 = sp^\ell + tu$．所以

$$x = (sp^\ell + tu)x = sp^\ell x + tux = 0.$$

（ⅱ）现在把刚才给出的证明翻译为模的语言．如果 $m \in M$ 是非零的，它的阶理想 $\operatorname{ann}(m) = (d)$，其中 $d \in R$．根据唯一因子分解，存在不可约元素 $p_1, \cdots, p_n$（它们中任两个都不是相伴的）

和正指数 $e_1,\cdots,e_n$ 使得

$$d = p_1^{e_1}\cdots p_n^{e_n}.$$

根据命题 6.17，对每个 i，$P_i=(p_i)$ 是素理想．定义 $r_i = d/p_i^{e_i}$，从而 $p_i^{e_i}r_i = d$．由此，对每个 i，$r_i m \in M_{P_i}$．但元素 $r_1,\cdots,r_n$ 的 gcd 是 1，从而存在元素 $s_1,\cdots,s_n \in R$ 使得 $1=\sum_i s_i r_i$．所以，

$$m = \sum_i s_i r_i m \in \left\langle \bigcup_P M_P \right\rangle.$$

对每个素理想 P，记 $H_P = \left\langle \bigcup_{Q\neq P} G_Q \right\rangle$．根据习题 7.79，只要证明如果

$$m \in M_P \cap H_P,$$

则 $m=0$．因 $m\in M_P$，其中 $P=(p)$，有某个 $\ell \geqslant 0$ 使得 $p^\ell m = 0$；因 $m \in H_P$，有 $um=0$，其中 $u = q_1^{f_1}\cdots q_n^{f_n}, Q_i=(q_i), f_i\geqslant 1$．但 p^ℓ 和 u 互素，因此存在 $s,t\in R$ 使得 $1 = sp^\ell + tu$．所以

$$m = (sp^\ell + tu)m = sp^\ell m + tum = 0. \qquad \blacksquare$$

命题 9.11 *PID 上的两个挠模 M 和 M' 同构当且仅当对每个非零素理想 P，$M_P \cong M'_P$．*

证明 如果 $f: M\to M'$ 是 R-映射，则对每个素理想 $P=(p)$，$f(M_P)\subseteq M'_P$，这是因为如果 $p^\ell m = 0$，则 $0 = f(p^\ell m) = p^\ell f(m)$．如果 f 是同构，则 $f^{-1}: M'\to M$ 也是同构．由此每个限制 $f\mid M_P : M_P \to M'_P$ 是同构，逆为 $f^{-1}\mid M'_P$．反之，如果对一切 P 存在同构 $f_P: M_P\to M'_P$，则存在同构 $\varphi: \sum_P M_P \to \sum_P M'_P$，它由 $\sum_P m_P \mapsto \sum_P f_P(m_P)$ 给出． $\blacksquare$

[653]

我们说明，和命题 9.2 一样，这里也有一个奇特的证明．定义"P-挠函子"$t_P: {}_R\mathbf{Mod}\to {}_R\mathbf{Mod}$，在模上为 $M\mapsto (tM)_P$，在态射上为 $\varphi \mapsto \varphi\mid(tM)_P$．由每个函子保持等价得 $(tM)_P \cong (tM')_P$．

对本节的剩下部分，我们仅给出定义和结果的陈述；读者不难修改关于阿贝尔群的定理的证明来证明关于 PID 上的模的定理．

定理 9.12（基定理） *如果 R 是 PID，则每个有限生成模 M 都是循环模的直和，其中每个循环直和项或者是准素的，或者同构于 R.*

证明 根据系 9.5，$M = tM \oplus F$，其中 F 是有限生成自由模；见定理 5.18 阿贝尔群的基定理. $\blacksquare$

注 *这里有基定理的一个精致的证明，可供读者欣赏．根据系 9.5 和定理 9.10(ii)，可以假定 M 是 P-准素的，其中 P 是某个素理想 $P=(p)$.*

存在正整数 e 使得 $p^eM=\{0\}$：如果 $M=\langle m_1,\cdots,m_n\rangle$，则有某个 e_i 使得 $p^{e_i}m_i = 0$，我们选取 e 为这些 e_i 中最大的一个（可以假定 $e=e_n$）．根据习题 7.4，如果 $J=(p^e)$，则 M/JM 是 R/J-模；其实，因 $JM=\{0\}$，M 自身就是一个 R/J-模．现在根据命题 7.76，$\langle m_n\rangle \cong R/(p^e) = R/J$ 是一个内射 R/J-模，命题 7.64 说子模 $S=\langle m_n\rangle$ 是直和项：

$$M = \langle m_n\rangle \oplus T,$$

其中 T 是 M 的 R/J-子模；更不必说 T 是 M 的 R-子模 [如果 $r\in R$ 和 $t\in T$，则 $(r+J)t$ 有意义；定义 $rt=(r+J)t$]．由于 T 可以由少于 n 个元素生成，因此可以用归纳法假定它是循环子模的直和．

系 9.13 *每个有限生成阿贝尔群是循环群的直和，这些直和的阶是素数的幂或无限．*

什么时候 PID 上的两个有限生成模 M 和 M' 同构？

开始陈述下一引理之前，回忆 M/pM 是 $R/(p)$ 上的向量空间，并且定义

$$d(M) = \dim(M/pM).$$

特别地，$d(pM) = \dim(pM/p^2M)$，更一般地，

$$d(p^nM) = \dim(p^nM/p^{n+1}M).$$

定义 如果 M 是有限生成(p)-准素 R-模，其中 R 是 PID 和 $P=(p)$是素理想，则

$$U_P(n,M) = d(p^nM) - d(p^{n+1}M).$$

654

定理 9.14 如果 R 是 PID 和 $P=(p)$ 是 R 中的素理想，则有限生成 P-准素 R-模 M 的任意两个循环模的直和分解中，每一类型的循环直和项的个数相等．精确地说，对每个 $n \geqslant 0$，阶理想为 (p^{n+1}) 的循环直和项的个数是 $U_P(n,M)$．

证明 见定理 5.23. ■

系 9.15 如果 M 和 M' 都是 P-准素 R-模，其中 R 是 PID，则$M \cong M'$ 当且仅当对一切 $n \geqslant 0, U_P(n,M) = U_P(n,M')$．

证明 见系 5.24. ■

定义 如果 M 是 P-准素 R-模，其中 R 是 PID，则 M 的**初等因子**是指理想 (p^{n+1})，且有重数 $U_P(n,M)$．

如果 M 是有限生成挠 R-模，则它的**初等因子**是指它的一切准素分量的初等因子．

下一定义是由系 5.30 引发的：如果 G 是有初等因子 $\{p_i^{e_{ij}}\}$ 的有限阿贝尔群，则

$$|G| = \prod_{ij} p_i^{e_{ij}}.$$

定义 如果 M 是有限生成挠 R-模，其中 R 是 PID，则 M 的**阶**是指由它的初等因子的积生成的主理想，就是 $\left(\prod_{ij} p_i^{e_{ij}}\right)$.

例 9.16 如果 k 是域，阶为 $(x-1)^3(x+1)^2$ 的 $k[x]$-模有多少？根据准素分解，阶为 $(x-1)^3(x+1)^2$ 的每个 $k[x]$-模是阶分别为 $(x-1)^3$ 和 $(x+1)^2$ 的准素模的直和．阶为 $(x-1)^3$ 的模有 3 个，用初等因子来描述是

$$(x-1, x-1, x-1), (x-1, (x-1)^2) \text{ 和 } (x-1)^3;$$

阶为 $(x+1)^2$ 的模有 2 个，用初等因子来描述是

$$(x+1, x+1) \text{ 和 } (x+1)^2.$$

所以如不计同构，阶为 $(x-1)^3(x+1)^2$ 的模有 6 个．

读者或许已注意到这个论证和例 5.26 中对 $72=2^3 3^2$ 阶阿贝尔群分类的论证相同． ■

655

定理 9.17（有限生成模的基本定理） 如果 R 是 PID，则两个有限生成 R-模同构当且仅当它们的挠子模有相同的初等因子且它们的自由部分有相同的秩．

证明 根据定理9.10(ii)，$M \cong M'$ 当且仅当对一切素理想 P，准素分量 M_P 和 M'_P 同构．现在可以用系 9.15、命题9.5(ii)和命题 9.11 完成证明． ■

下面是有限生成挠模的另一种类型的分解，它也是分解为循环模的直和，但没有提及准素模．

命题 9.18 如果 R 是 PID，则每个有限生成挠 R-模都是循环模的直和

$$M = R/(c_1) \oplus R/(c_2) \oplus \cdots \oplus R/(c_t),$$

其中 $t \geqslant 1$ 和 $c_1 \mid c_2 \mid \cdots \mid c_t$.

证明 见命题 5.27. ■

定义 如果 M 是有限生成挠 R-模，其中 R 是 PID，又如果

$$M = R/(c_1) \oplus R/(c_2) \oplus \cdots \oplus R/(c_t),$$

其中 $t \geqslant 1$ 和 $c_1 \mid c_2 \mid \cdots \mid c_t$，则 $(c_1), (c_2), \cdots, (c_t)$ 称为 M 的**不变因子**.

系 9.19 如果 M 是 PID 上的有限生成挠模，则

$$(c_t) = \{r \in R : rM = \{0\}\},$$

其中 (c_t) 是命题 9.18 中 M 的分解中出现的最后一个理想.

特别地，如果 $R = k[x]$，其中 k 是域，则 c_t 是满足 $c_t M = \{0\}$ 的次数最小的多项式.

证明 第一个陈述见系 5.28.

第二个陈述来自下列事实：$k[x]$ 中的每个非零理想由其中次数最小的首一多项式生成. ■

定义 如果 M 是 R-模，则它的**指数**（或**零化子**）是指理想

$$\operatorname{ann}(M) = \{r \in R : rM = \{0\}\}.$$

[656] 系 9.19 计算了 PID 上有限生成挠模的指数，它是最后一个不变因子 (c_t).

系 9.20 如果 M 是有不变因子 $c_1, \cdots, c_t$ 的有限生成挠 R-模，其中 R 是 PID，则 M 的阶是 $\left(\prod_{i=1}^{t} c_i\right)$.

证明 见系 5.30. 读者应验证由初等因子的积（它被定义为 M 的阶）生成的主理想等于主理想 $\left(\prod_{i=1}^{t} c_i\right)$. ■

例 9.21 例 9.16 给出了阶为 $(x-1)^3(x+1)^2$ 的 $k[x]$-模的初等因子，下面是它们的不变因子.

初等因子 $\leftrightarrow$ 不变因子

$$(x-1, x-1, x-1, x+1, x+1) \leftrightarrow x-1 \mid (x-1)(x+1) \mid (x-1)(x+1)$$
$$(x-1, (x-1)^2, x+1, x+1) \leftrightarrow (x-1)(x+1) \mid (x-1)^2(x+1)$$
$$((x-1)^3, x+1, x+1) \leftrightarrow x+1 \mid (x-1)^3(x+1)$$
$$(x-1, x-1, x-1, (x+1)^2) \leftrightarrow x-1 \mid x-1 \mid (x-1)(x+1)^2$$
$$(x-1, (x-1)^2, (x+1)^2) \leftrightarrow x-1 \mid (x-1)^2(x+1)^2$$
$$((x-1)^3, (x+1)^2) \leftrightarrow (x-1)^3(x+1)^2$$

■

定理 9.22（不变因子） 如果 R 是 PID，则两个有限生成 R-模同构当且仅当它们的挠子模有相同的不变因子且它们的自由部分有相同的秩.

证明 根据系 9.5(i)，每个有限生成 R-模 M 是直和 $M = tM \oplus F$，其中 F 是自由的，且 $M \cong M'$ 当且仅当 $tM \cong tM'$ 和 $F \cong F'$. 系 9.5(ii)表明自由部分 $F \cong M/tM$ 和 $F' \cong M'/tM'$ 是同构的，定理 5.32 的简单推广证明挠子模是同构的. ■

读者现在应该习惯于我们的说明：一个定理可以容易地从阿贝尔群推广到 PID 上的模. 接下来，我们将只对阿贝尔群陈述和证明定理，而把到模上的简单推广留给读者.

考虑非有限生成的模. 回忆一个阿贝尔群 D 是**可除的**，如果对每个 $d \in D$ 和每个正整数 n，存在 $d' \in D$ 使得 $d = nd'$. 可除群的每个商是可除群，可除群的直和是可除群. 现在系 7.73 说一个阿贝尔群 D 是一个内射$\mathbb{Z}$-模当且仅当它是可除的，从而可除群的分类描述了一切内射阿贝尔群.

[657] **命题 9.23** 无挠阿贝尔群 D 是可除的当且仅当它是$\mathbb{Q}$上的向量空间.

证明 如果 D 是$\mathbb{Q}$上的向量空间，则它是$\mathbb{Q}$的复制的直和，这是因为每个向量空间都有基. 但$\mathbb{Q}$是可除群，而可除群的任一直和是可除群.

设 D 是无挠的和可除的；我们需要证明 D 接纳有理数的标量乘法．假设 $d\in D$ 和 n 是正整数．因 D 是可除的，存在 $d'\in D$ 使得 $nd'=d$ ［当然，d'是 $(1/n)d$ 的候选者］．注意，因 D 是无挠的，d'是唯一的这样的元素：如果还有 $nd''=d$，则 $n(d'-d'')=0$，从而 $d'-d''$ 有有限阶，因此是 0．如果 $m/n\in\mathbb{Q}$，定义 $(m/n)d=md'$，其中 $nd'=d$．证明这个标量乘法是合理定义的［如果 $m/n=a/b$，则 $(m/n)d=(a/b)d$］和向量空间定义中的各公理成立只是留给读者的一个简单练习． ■

定义 如果 G 是阿贝尔群，则 dG 是由 G 的一切可除子群生成的子群．

命题 9.24 （ⅰ）对每个阿贝尔群 G，子群 dG 是 G 的唯一极大可除子群．

（ⅱ）每个阿贝尔群 G 是直和

$$G=dG\oplus R.$$

其中 $dR=\{0\}$．因此，$R\cong G/dG$ 没有非零可除子群．

证明 （ⅰ）只需证明 dG 是可除的，因为它是可除的就必是最大的可除子群．如果 $x\in dG$，则 $x=x_1+\cdots+x_t$，其中 $x_i\in D_i$，D_i 是 G 的可除子群．如果 n 是正整数，则因为 D_i 是可除的，存在 $y_i\in D_i$ 使得 $x_i=ny_i$．从而 $y=y_1+\cdots+y_t\in dG$ 和 $x=ny$，因此 dG 是可除的．

（ⅱ）因 dG 是可除的，所以它是内射的，命题 7.64 给出

$$G=dG\oplus R,$$

其中 R 是 G 的子群．如果 R 有非零可除子群 D，则根据命题 7.64，有某个子群 S 使得 $R=D\oplus S$．但 $dG\oplus D$ 是 G 的真包含 dG 的可除子群，与（ⅰ）矛盾．

定义 称阿贝尔群为**约化的**，如果 $dG=\{0\}$；即 G 没有非零可除子群．

习题 9.18 中，我们证明阿贝尔群 G 是约化的当且仅当 $\mathrm{Hom}(\mathbb{Q},G)=\{0\}$．

我们刚才已经证明了 G/dG 总是约化的．读者应该把群 G 的极大可除子群 dG 和它的挠子群 tG 作一比较：如果 $tG=G$，G 是挠的，如果 $tG=\{0\}$，G 是无挠的；如果 $dG=G$，G 是可除的，如果 $dG=\{0\}$，G 是约化的．存在正合列 [658]

$$0\to dG\to G\to G/dG\to 0$$

和

$$0\to tG\to G\to G/tG\to 0;$$

第一个序列恒分裂，但在习题 9.1（ⅲ）中将看到第二个序列可能不分裂．

下面的群有一些值得注意的性质．

定义 如果 p 是素数，复数 z 称为 p **幂次单位根**，如果有某个 $n\geq 1$ 使得 $z^{p^n}=1$．**拟循环群**（也称 p^∞ 型普吕弗（Prüfer）群）是指

$$\mathbb{Z}(p^\infty)=\{\text{复 } p \text{ 幂次单位根}\}.$$

当然，如果 z 是 p 幂次单位根，比如 $z^{p^n}=1$，则 z 是 p^n 次单位原根 $z_n=e^{2\pi i/p^n}$ 的幂．注意，对每个整数 $n\geq 1$，子群 $\langle z_n\rangle$ 是 $\mathbb{Z}(p^\infty)$ 的唯一 p^n 阶子群，这是因为多项式 $x^{p^n}-1\in\mathbb{C}[x]$ 至多有 p^n 个复根．

命题 9.25 设 p 是素数．

（ⅰ）$\mathbb{Z}(p^\infty)$ 同构于 $\mathbb{Q}/\mathbb{Z}$ 的 p-准素分量．

（ⅱ）$\mathbb{Z}(p^\infty)$ 是可除 p-准素阿贝尔群．

（ⅲ）$\mathbb{Z}(p^\infty)$ 的子群是

$$\{1\}\subsetneq\langle z_1\rangle\subsetneq\langle z_2\rangle\subsetneq\cdots\subsetneq\langle z_n\rangle\subsetneq\langle z_{n+1}\rangle\subsetneq\cdots\subsetneq\mathbb{Z}(p^\infty),$$

因此它们由包含形成良序集．[⊖]

(iv) $\mathbb{Z}(p^{\infty})$ 有子群上的 DCC，但没有 ACC．[⊜]

证明 (i) 定义 $\sum_p \mathbb{Z}(p^{\infty}) \to \mathbb{Q}/\mathbb{Z}$ 为 $(e^{2\pi i c_p/p^{n_p}}) \mapsto \sum_p c_p/p^{n_p} + \mathbb{Z}$，其中 $c_p \in \mathbb{Z}$．易知 φ 是单同态．φ 是满射的证明其实已包含在定理 5.13 的证明中，但这里再做一次．设 $a/b \in \mathbb{Q}/\mathbb{Z}$，并记 $b = \prod_p p^{n_p}$．因为数 b/p^{n_p} 是两两互素的，存在整数 m_p 使得 $1 = \sum_p m_p(b/p^{n_p})$．所以，$a/b = \sum_p am_p/p^{n_p} = (\varphi(e^{a2\pi i m_p/p^{n_p}}))$．

659

(ii) 因直和项恒为同态象，所以 $\mathbb{Z}(p^{\infty})$ 是可除群 $\mathbb{Q}/\mathbb{Z}$ 的同态象；但可除群的商也是可除的．

(iii) 设 S 是 $\mathbb{Z}(p^{\infty})$ 的真子群．因 $\{z_n : n \geqslant 1\}$ 生成 $\mathbb{Z}(p^{\infty})$，我们可以假定有某个 m 使得 $z_m \notin S$．由此对一切 $\ell > m, z_\ell \notin S$；否则 $z_m = z_\ell^{p^{\ell-m}} \in S$．如果 $S \neq \{0\}$，我们断言 S 包含某个 z_n；事实上，我们证明 S 包含 z_1．现在 S 必包含某个 p 阶元素 x，而 $x = z_1^c$，其中 $1 \leqslant c < p$ [因为 $\langle z_1 \rangle$ 包含 $\mathbb{Z}(p^{\infty})$ 中的一切 p 阶元素]．因 p 是素数，$(c,p)=1$，存在整数 u，v 使得 $1 = cu + pv$；因此，$z_1 = z_1^{cu+pv} = z_1^{cu} = x^u \in S$．设 d 是使得 $z_d \in S$ 的最大整数．显然 $\langle z_d \rangle \subseteq S$．关于反包含，设 $s \in S$．如果 s 有阶 $p^n > p^d$，则 $\langle s \rangle$ 包含 z_n，这是因为 $\langle z_n \rangle$ 包含 $\mathbb{Z}(p^{\infty})$ 中的一切 p^n 阶元素．但这与对一切 $\ell > d$ 有 $z_\ell \notin S$ 的观察矛盾．因此，s 的阶 $\leqslant p^d$，从而 $s \in \langle z_d \rangle$；所以，$S = \langle z_d \rangle$．

由于 $\mathbb{Z}(p^{\infty})$ 的非零真子群只有 $\langle z_n \rangle$，所以子群由包含关系形成良序．

(iv) 首先，$\mathbb{Z}(p^{\infty})$ 没有 ACC，这由子群链

$$\{1\} \subsetneq \langle z_1 \rangle \subsetneq \langle z_2 \rangle \subsetneq \cdots$$

得以说明．附录的命题 A.3 证明了良序集中的严格递减序列是有限的；因此 $\mathbb{Z}(p^{\infty})$ 在子群上有 DCC. ■

记号 如果 G 是阿贝尔群和 n 是正整数，则

$$G[n] = \{g \in G : ng = 0\}.$$

易知 $G[n]$ 是 G 的子群．注意，如果 p 是素数，则 $G[p]$ 是 $\mathbb{F}_p$ 上的向量空间．

引理 9.26 如果 G 和 H 都是可除 p-准素阿贝尔群，则 $G \cong H$ 当且仅当 $G[p] \cong H[p]$.

证明 如果存在同构 $f: G \to H$，则易知它的限制 $f \mid G[p]$ 是同构 $G[p] \to H[p]$（它的逆是 $f^{-1} \mid H[p]$）．

关于充分性，假设 $f: G[p] \to H[p]$ 是同构．结合包含映射 $H[p] \to H$，可以假定 $f: G[p] \to H$．因 H 是内射的，所以 f 可以扩张为同态 $F: G \to H$；我们断言任意这样的 F 都是同构．

(i) F 是单射．

如果 $g \in G$ 有阶 p，则根据假设，$F(g) = f(g) \neq 0$．假定 g 有阶 $p^n, n \geqslant 2$．如果 $F(g) = 0$，则 $F(p^{n-1}g) = 0$，这与假设矛盾，因为 $p^{n-1}g$ 有阶 p. 所以 F 是单射．

(ii) F 是满射．

对 $n \geqslant 1$ 用归纳法证明．如果 $h \in H$ 有阶 p^n，则 $h \in \operatorname{im} F$．如果 $n=1$，则 $h \in H[p] = \operatorname{im} f \subseteq$

⊖ 群 $\mathbb{Z}(p^{\infty})$ 叫做拟循环的是因为它的每个真子群都是循环的．

⊜ 定理 8.46，即霍普金斯-列维茨基（Hopkins-Levitzki）定理说有 DCC 的环必有 ACC. 这一结果表明类似的结果对群不成立．

$\mathrm{im}F$. 关于归纳步，假定 $h \in H$ 有阶 p^{n+1}. 现在 $p^n h \in H[p]$，因此存在 $g \in G$ 使得 $F(g) = f(g) = p^n h$. 因 G 是可除的，存在 $g' \in G$ 使得 $p^n g' = g$；于是，$p^n(h - F(g')) = 0$. 根据归纳假设，存在 $x \in G$ 使得 $F(x) = h - F(g')$. 所以正如所要的，$F(x + g') = h$. ■ 660

下一定理将一切可除阿贝尔群分类.

定义 如果 D 是可除阿贝尔群，定义

$$\delta_\infty(D) = \dim_{\mathbb{Q}}(D/tD),$$

并对一切素数 p，定义

$$\delta_p(D) = \dim\mathbb{F}_p(D[p]).$$

定理 9.27 (i) 阿贝尔群 D 是内射$\mathbb{Z}$-模当且仅当它是可除群.

(ii) 可除阿贝尔群同构于一个$\mathbb{Q}$的复制的直和和$\mathbb{Z}(p^\infty)$的复制的直和，其中 p 是不同的素数.

(iii) 两个可除群 D 和 D' 同构当且仅当 $\delta_\infty(D) = \delta_\infty(D')$ 和对一切素数 p，$\delta_p(D) = \delta_p(D')$.

证明 (i) 在系 7.73 中已经得到证明.

(ii) 如果 $x \in D$ 的阶有限，n 是正整数，又如果 $x = ny$，则 y 的阶有限. 从而如果 D 是可除的，则它的挠子群 tD 也是可除的，因此

$$D = tD \oplus V,$$

其中 V 是无挠的（根据命题 7.64）. 因可除群的商是可除的，V 是无挠的和可除的，因此根据命题 9.23，它是$\mathbb{Q}$上的向量空间.

现在 tD 是它的准素分量的直和：$tD = \sum_p T_p$，其中每个直和项是 p-准素的和可除的，因此只要证明每个 T_p 是$\mathbb{Z}(p^\infty)$的复制的直和. 如果 $\dim(T_p[p]) = r$（r 可以无限），定义 W 为$\mathbb{Z}(p^\infty)$的 r 个复制的直和，从而 $\dim(W[p]) = r$. 现在引理 9.26 表明 $T_p \cong W$.

(iii) 根据命题 9.2(ii)，如果 $D \cong D'$，则 $D/tD \cong D'/tD'$ 和 $tD \cong tD'$；因此对一切 p，p-准素分量 $(tD)_p \cong (tD')_p$. 但 D/tD 和 D'/tD' 是$\mathbb{Q}$上同构的向量空间，因此有相同的维数；此外，向量空间 $(tD)_p[p]$ 和 $(tD')_p[p]$ 也是同构的，从而它们也有相同的维数.

关于逆命题，记 $D = V \oplus \sum_p T_p$ 和 $D' = V' \oplus \sum_p T'_p$，其中 V 和 V' 是无挠可除的，T_p 和 T'_p 是 p-准素可除的. 根据引理 9.26，$\delta_p(D') = \delta_p(D')$ 蕴涵 $T_p \cong T'_p$，而 $\delta_\infty(D) = \delta_\infty(D')$ 蕴涵向量空间 V 和 V' 同构. 根据命题 7.30，以上同构能够组合为 D 和 D' 之间的同构. ■

我们现在可以描述一些熟悉的群，但读者必须复习一点域论的知识. 661

系 9.28 设 k 是代数闭域，$k^\times$ 是它的乘法群，并设 T 是 $k^\times$ 的挠群.

(i) 如果 k 有特征 0，则 $T \cong \mathbb{Q}/\mathbb{Z}$ 和 $k^\times \cong (\mathbb{Q}/\mathbb{Z}) \oplus V$，其中 V 是$\mathbb{Q}$上的向量空间.

(ii) 如果 k 的特征为素数 p，则 $T \cong \sum_{q \neq p} \mathbb{Z}(q^\infty)$. 如果 k 是$\mathbb{F}_p$ 的代数闭包，则[㊀]

$$k^\times \cong \sum_{q \neq p} \mathbb{Z}(q^\infty).$$

证明 因 k 是代数闭域，只要 $a \in k$，多项式 $x^n - a$ 在 k 中就必有根；这就是说每个 a 在 k 中都有 n 次根，这是用乘法的方式说 $k^\times$ 是可除群. 元素 $a \in k$ 的阶有限当且仅当有某个正整数 n 使得 $a^n = 1$；即 a 是一个 n 次单位根. 易知 T 自身是可除的. 因此根据引理 9.24，$k^\times = T \oplus V$，其中 V 是$\mathbb{Q}$上的向量空间（因为 V 是无挠可除的）.

㊀ 容易描述 k 的加法群，因为 k 是$\mathbb{F}_p$ 上的向量空间，因此它是$\mathbb{F}_p$ 的（无限个）复制的直和.

（ⅰ）如果 $k=\overline{\mathbb{Q}}$ 是 $\mathbb{Q}$ 的代数闭包，不失一般性可假定 $k\subseteq\mathbb{C}$. 现在 k 的挠子群 T 由一切单位根 $e^{2\pi ir}$ 组成，其中 $r\in\mathbb{Q}$. 由此易知映射 $r\mapsto e^{2\pi ir}$ 是以 $\mathbb{Z}$ 为核的满射 $\mathbb{Q}\to T$，因此 $T\cong\mathbb{Q}/\mathbb{Z}$.

如果 k 是任一特征为 0 的代数闭域，则 $\mathbb{Q}\subseteq k$ 蕴涵 $\overline{\mathbb{Q}}\subseteq k$. 因为 $\overline{\mathbb{Q}}$ 已经包含了 x^n-1 的 n 个根，所以不可能有单位根在 k 中而不在 $\overline{\mathbb{Q}}$ 中.

（ⅱ）设 $k=\overline{\mathbb{F}}_p$. 每个元素 $a\in k$ 是 $\mathbb{F}_p$ 上的代数元素，因此 $\mathbb{F}_p(a)/\mathbb{F}_p$ 是有限域扩张；比如对某个 m 有 $[\mathbb{F}_p(a):\mathbb{F}_p]=m$. 因此，$|\mathbb{F}_p(a)|=p^m$ 和 $\mathbb{F}_p(a)$ 是有限域. 现在有限域中的每个非零元素都是单位根（因为它是 $x^{p^m}-x$ 关于某个 m 的根）. 但 $k^\times=T\oplus V$，其中 V 是 $\mathbb{Q}$ 上的向量空间. 由此，$V=\{0\}$，这是因为 k 中的每个非零元素都是单位根.

我们现在考察 $k^\times$ 的准素分量. 如果 $q\neq p$ 是素数，则多项式 $f(x)=x^q-1$ 没有重根（因为 $\gcd(f(x),f'(x))=1$），因此有某个不同于 1 的 q 次单位根. 于是，$k^\times$ 的 q-准素分量是非平凡的，因此至少有一个直和项同构于 $\mathbb{Z}(q^\infty)$. 要是这种直和项多于一个，那么 q 阶元素就多于 q 个，这样，x^q-1 在域 k 中便有太多的根. 最后，因为在 $k[x]$ 中多项式 $x^p-1=(x-1)^p$，因此没有不同于 1 的根，所以没有直和项同构于 $\mathbb{Z}(p^\infty)$. ■

系 9.29 下列阿贝尔群同构：

662

$$\mathbb{C}^\times;(\mathbb{Q}/\mathbb{Z})\oplus\mathbb{R};\mathbb{R}/\mathbb{Z};\prod_p\mathbb{Z}(p^\infty);S^1.$$

这里 S^1 是圆群；即它是满足 $|z|=1$ 的一切复数 z 的乘法群.

证明 列出的每个群 G 对每个素数 p 有 $\delta_p(G)=1$ 和 $\delta_\infty(G)=c$（连续统的基数），因此读者可以运用定理 9.27. 对于 $G=\prod_p\mathbb{Z}(p^\infty)$，见习题 9.29. ■

习题

9.1 设 $G=\prod_p\langle a_p\rangle$，其中 p 遍历一切素数，且 $\langle a_p\rangle\cong\mathbb{I}_p$.

（ⅰ）证明 $tG=\sum_p\langle a_p\rangle$.

提示：用习题 5.4.

（ⅱ）证明 G/tG 是可除群.

（ⅲ）证明 tG 不是 G 的直和项.

提示：证明 $\mathrm{Hom}(\mathbb{Q},G)=\{0\}$，但 $\mathrm{Hom}(\mathbb{Q},G/tG)\neq\{0\}$，由此推出 G/tG 不能同构于 G 的子群.

9.2 设 R 是 PID，并设 M 是 R-模，不必准素. 定义子模 $S\subseteq M$ 为**纯子模**，如果对一切 $r\in R$ 有 $S\cap rM=rS$.

（ⅰ）证明：如果 M 是 (p)-准素模，其中 (p) 是 R 中的非零素理想，则子模 $S\subseteq M$ 是纯子模当且仅当对一切 $n\geqslant 0$，$S\cap p^nM=p^nS$.

（ⅱ）证明 M 的每个直和项都是纯子模.

（ⅲ）证明挠子模 tM 是 M 的纯子模.

（ⅳ）证明：如果 M/S 是无挠的，则 S 是 M 的纯子模.

（ⅴ）证明：如果 $\mathcal{S}$ 是模 M 的纯子模的族，且在包含关系下形成链（即如果 $S,S'\in\mathcal{S}$，则 $S\subseteq S'$ 或 $S'\subseteq S$），则 $\bigcup_{s\in\mathcal{S}}S$ 是 M 的纯子模.

（ⅵ）举出一个不是直和项的纯子模的例子.

9.3 （ⅰ）如果 F 是有限生成自由 R-模，其中 R 是 PID，证明 F 的每个纯子模都是直和项.

（ⅱ）如果 R 是 PID 和 M 是有限生成 R-模，证明子模 $S\subseteq M$ 是 M 的纯子模当且仅当 S 是 M 的直和项．

9.4 证明：如果 R 是整环而不是域，则既是投射的又是内射的 R-模 M 必是$\{0\}$.

提示：用习题 7.43.

9.5 如果 M 是整环 R 上的挠模，证明

$$\mathrm{Hom}_R(M,M)\cong\prod_P \mathrm{Hom}_R(M_P,M_P),$$

其中 M_P 是 M 的 P-准素分量．

9.6 （ⅰ）如果 G 是挠群，它有 p-准素分量 $\{G_p:p\in P\}$，其中 P 是一切素数的集合，证明 $G=t(\prod_{p\in P}G_p)$.

（ⅱ）证明 $(\prod_{p\in P}G_p)/(\sum_{p\in P}G_p)$ 是无挠的和可除的．

提示：用习题 5.4.

663

9.7 如果 M 是 R-模，其中 R 是整环，又如果 $r\in R$，设 $\mu_r:M\to M$ 是乘 r 的映射；即 $\mu_r:m\mapsto rm$ [见例 7.2（ⅲ）]．

（ⅰ）如果 $Q=\mathrm{Frac}(R)$，证明 R-模 M 是 Q 上的向量空间当且仅当 M 是无挠的和可除的．

（ⅱ）证明对每个 $r\neq 0$，μ_r 都是单射当且仅当 M 是无挠的．

（ⅲ）证明对每个 $r\neq 0$，μ_r 都是满射当且仅当 M 是可除的．

（ⅳ）证明 M 是 Q 上的向量空间当且仅当对每个 $r\neq 0$，映射 $\mu_r:M\to M$ 是同构．

9.8 （ⅰ）设 R 是整环，$r\in R$，并设 M 是 R-模．如果 $\mu_r:M\to M$ 是乘 r 的映射，证明对每个 R-模 A，诱导映射

$$(\mu_r)_*:\mathrm{Hom}_R(A,M)\to\mathrm{Hom}_R(A,M)$$

和

$$(\mu_r)^*:\mathrm{Hom}_R(M,A)\to\mathrm{Hom}_R(M,A)$$

也是乘 r 的映射．

（ⅱ）设 R 是整环，且 $Q=\mathrm{Frac}(R)$．用习题 9.7 证明对每个 R-模 M，$\mathrm{Hom}_R(Q,M)$ 和 $\mathrm{Hom}_R(M,Q)$ 都是 Q 上的向量空间．

9.9 （ⅰ）如果 M 和 N 都是有限生成挠 R-模，证明对一切素理想 P 和一切 $n\geqslant 0$，

$$U_P(n,M\oplus N)=U_P(n,M)+U_P(n,N),$$

（ⅱ）如果 A，B 和 C 都是有限生成 R-模，其中 R 是 PID，证明 $A\oplus B\cong A\oplus C$ 蕴涵 $B\cong C$.

（ⅲ）如果 A 和 B 都是有限生成 R-模，其中 R 是 PID，证明 $A\oplus A\cong B\oplus B$ 蕴涵 $A\cong B$.

9.10 如果 A 是阿贝尔群，则 A 的子集 X 称为**线性无关**，只要 $\sum_i m_ix_i=0$，其中 $m_i\in\mathbb{Z}$ 且几乎一切 $m_i=0$，则对一切 i，$m_i=0$．定义 $\mathrm{rank}(A)$ 为 A 的极大线性无关子集中元素的个数．

（ⅰ）如果 X 线性无关，证明 $\langle X\rangle=\sum_{x\in X}\langle x\rangle$，即循环群的直和．

（ⅱ）如果 A 是挠的，证明 $\mathrm{rank}(A)=0$.

（ⅲ）如果 A 是自由阿贝尔群，证明两个秩的概念一致［早先的概念定义 $\mathrm{rank}(A)$ 为 A 的基中元素的个数］．

（ⅳ）证明 $\mathrm{rank}(A)=\dim(\mathbb{Q}\otimes_{\mathbb{Z}}A)$，由此推出 A 的每两个极大线性无关子集的元素个数相等；即 $\mathrm{rank}(A)$ 是合理定义的．

（ⅴ）如果 $0\to A\to B\to C\to 0$ 是阿贝尔群的正合列，证明 $\mathrm{rank}(B)=\mathrm{rank}(A)+\mathrm{rank}(C)$.

9.11 (Kulikov) 如果 G 是阿贝尔 p-群，称子集 $X\subseteq G$ 为**纯无关的**，如果 X 是线性无关的（见习题 9.10）且 $\langle X\rangle$ 是纯子群．

（ⅰ）证明 G 有极大纯无关子集．

（ⅱ）如果 X 是 G 的极大纯无关子集，则子群 $B=\langle X\rangle$ 叫做 G 的**基本子群**．证明：如果 B 是 G 的基本子群，则 G/B 是可除的．

9.12 证明：如果 G 和 H 都是挠阿贝尔群，则 $G\otimes_{\mathbb{Z}}H$ 是循环群的直和．

提示：用正合列 $0\to B\to G\to G/B\to 0$（其中 B 是基本子群）以及 Rotman 所著的《An Introduction to

664

Homological Algebra》94～96 页中证明的下列定理：如果 $0\to A'\xrightarrow{i}A\to A''\to 0$ 是阿贝尔群的正合列，且 $i(A')$ 是 A 的纯子群，则对每个阿贝尔群 E，

$$0\to A'\oplus_{\mathbb{Z}}E\to A\otimes_{\mathbb{Z}}E\to A''\otimes_{\mathbb{Z}}E\to 0$$

是正合的．

9.13 设 M 是 P-准素 R-模，其中 R 是 PID 和 $P=(p)$ 是素理想．对一切 $n\geqslant 0$，定义

$$V_P(n,M)=\dim\Big((p^nM\cap M[p])/(p^{n+1}M\cap M[p])\Big),$$

其中 $M[p]=\{m\in M: pm=0\}$．（因为不能减去无限基数，所以引入这个不变量．）

（ⅰ）证明当 M 有限生成时，$V_P(n,M)=U_P(n,M)$．

（ⅱ）设 $M=\sum_{i\in I}C_i$ 是循环模 C_i 的直和，其中 I 是任意指标集，可以无限．证明有阶理想 (p^n) 的直和项 C_i 的个数是 $V_P(n,M)$，因此它是 M 的一个不变量．

（ⅲ）设 M 和 M' 都是挠模，且都是循环模的直和．证明 $M\cong M'$ 当且仅当对一切 $n\geqslant 0$ 和一切素理想 P，$V_P(n,M)=V_P(n,M')$．

9.14 （ⅰ）如果 p 是素数和 $G=t\big(\prod_{k\geqslant 1}\langle a_k\rangle\big)$，其中 $\langle a_k\rangle$ 是 p^k 阶循环群，证明 G 是不可数 p-准素阿贝尔群，且对一切 $n\geqslant 0$，$V_p(n,G)=1$．

（ⅱ）用习题 9.13 证明（ⅰ）中的准素群 G 不是循环群的直和．

9.15 推广命题 8.95 如下：如果 R 是整环，D 是可除 R-模，T 是每个元素的阶都有限的挠 R-模，则 $D\otimes_R T=\{0\}$．

9.16 证明存在加性函子 $d:\mathbf{Ab}\to\mathbf{Ab}$ 把每个群 G 指派给它的极大可除子群 dG.

9.17 （ⅰ）证明 $\mathbb{Z}(p^\infty)$ 没有极大子群．

（ⅱ）证明 $\mathbb{Z}(p^\infty)\cong\varinjlim \mathbb{I}_{p^n}$．

（ⅲ）证明 $\mathbb{Z}(p^\infty)$ 的一个表现是

$$(a_n,n\geqslant 1\mid pa_1=0,\text{对一切 } n\geqslant 1, pa_{n+1}=a_n).$$

9.18 证明阿贝尔群 G 是约化的当且仅当 $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q},G)=\{0\}$.

9.19 如果 $0\to A\to B\to C\to 0$ 是正合列，且 A 和 C 都是约化的，证明 B 是约化的．

提示：用 $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q},\ )$ 的左正合性．

9.20 如果 $\{D_i: i\in I\}$ 是可除阿贝尔群的族，证明 $\prod_{i\in I}D_i$ 同构于可除群的一个直和．

9.21 证明 $\mathbb{Q}^\times\cong\mathbb{I}_2\oplus F$，其中 F 是无限秩的自由阿贝尔群．

9.22 证明 $\mathbb{R}^\times\cong\mathbb{I}_2\oplus\mathbb{R}$．

提示：用 e^x．

9.23 （ⅰ）证明对每个群同态 $f:\mathbb{Q}\to\mathbb{Q}$，存在 $r\in\mathbb{Q}$ 使得对一切 $x\in\mathbb{Q}$ 有 $f(x)=rx$．

（ⅱ）证明 $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Q})\cong\mathbb{Q}$．

（ⅲ）证明：作为环，$\mathrm{End}(\mathbb{Q})\cong\mathbb{Q}$．

665

9.24 对每个阿贝尔群 A，证明 $\mathrm{Hom}_{\mathbb{Z}}(A,\mathbb{Q})$ 和 $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q},A)$ 都是 $\mathbb{Q}$ 上的向量空间．

9.25　证明：如果 G 是非零阿贝尔群，则 $\mathrm{Hom}_{\mathbb{Z}}(G,\mathbb{Q}/\mathbb{Z})\neq\{0\}$.

9.26　证明阿贝尔群 G 是内射的当且仅当每个非零商群都是无限的.

9.27　证明：如果 G 是一切真子群都有限的无限阿贝尔群，则有某个素数 p 使得 $G\cong\mathbb{Z}(p^{\infty})$.[⊖]

9.28　（ⅰ）设 $D=\sum_{i=1}^{n}D_i$，其中每个 $D_i\cong\mathbb{Z}(p_i^{\infty})$，$p_i$ 是某个素数．证明 D 的每个子群都有 DCC.

（ⅱ）证明逆命题：如果阿贝尔群 G 有 DCC，则 G 同构于有限个 $\mathbb{Z}(p_i^{\infty})$ 的复制的直和的子群.

9.29　设 $G=\prod_{p\in P}\mathbb{Z}(p^{\infty})$，其中 P 是一切素数的集合．证明对一切 $p\in P$，$\delta_p(G)=1$，且 $\delta_\infty(G)=c$，其中 c 是连续统的基数.

提示：注意 $\prod_{p\in P}\mathbb{Z}(p^{\infty})$ 的基数为 c，而 $\sum_{p\in P}\mathbb{Z}(p^{\infty})$ 是可数的，然后用习题 9.6.

9.30　设 $R=k[x,y]$ 是域 k 上的二元多项式环，并设 $I=(x,y)$.

（ⅰ）证明在 $I\otimes_R I$ 中 $x\otimes y-y\otimes x\neq 0$.

提示：证明这些元素在 $(I/I^2)\otimes_R(I/I^2)$ 中有非零的象.

（ⅱ）证明 $x\otimes y-y\otimes x$ 是 $I\otimes_R I$ 中的挠元素，由此推出无挠模的张量积未必是无挠的.

9.31　设 $\mathcal{C}$ 是一切有限生成 R-模的范畴，其中 R 是 PID.

（ⅰ）计算格罗滕迪克群 $K_0(\mathcal{C})$.

（ⅱ）计算格罗滕迪克群 $K'(\mathcal{C})$.

9.2　有理典范型

在第 3 章中我们看到，如果 $T:V\to V$ 是线性变换，且 $X=x_1,\cdots,x_n$ 是 V 的基，则 T 确定矩阵 $A={}_X[T]_X$，它的第 i 列由 $T(x_i)$ 关于 X 的坐标集组成．如果 Y 是 V 的另一组基，则矩阵 $B={}_Y[T]_Y$ 可能与 A 不同，另一方面，系 3.101 说两个矩阵 A 和 B 由同一线性变换形成当且仅当 A 和 B 相似；即存在非奇异矩阵 P 使得 $B=PAP^{-1}$.

系 3.101　*设 $T:V\to V$ 是域 k 上的向量空间 V 上的线性变换．如果 X 和 Y 都是 V 的基，则存在元素在 k 中的非奇异矩阵 P 使得*

$$_Y[T]_Y=P({}_X[T]_X)P^{-1}.$$

反之，如果 $B=PAP^{-1}$，其中 B，A 和 P 都是元素在 k 中的 $n\times n$ 矩阵且 P 是非奇异的，则存在线性变换 $T:k^n\to k^n$ 和 k^n 的基 X 和 Y 使得 $B={}_Y[T]_Y$ 和 $A={}_X[T]_X$.

我们现在考虑如何确定给定的两个矩阵是否相似.　666

例 9.30　回忆例 7.1（ⅴ）：如果 $T:V\to V$ 是线性变换，其中 V 是域 k 上的向量空间，则 V 接纳由多项式 $f(x)\in k[x]$ 形成的标量乘法：

$$f(x)v=\Big(\sum_{i=0}^{m}c_ix^i\Big)v=\sum_{i=0}^{m}c_iT^i(v),$$

其中 T^0 是恒等映射 1_V．如果 $i\geqslant 1$，则 T^i 是 T 和它自己复合 i 次．记这个 $k[x]$-模为 V^T.

我们现在证明：如果 V 是 n 维的，则 $k[x]$-模 V^T 是一个挠模．根据系 3.88，对每个 $v\in V$，表 v，$T(v)$，$T^2(v)$，…，$T^n(v)$ 必是线性相关的（因为它包含 $n+1$ 个向量）．所以，存在不全为 0 的 $c_i\in k$ 使得 $\sum_{i=1}^{n}c_iT^i(v)=0$；但这说明 $g(x)=\sum_{i=0}^{n}c_ix^i$ 在阶理想 $\mathrm{ann}(v)$ 中. ■

⊖　存在一切真子群都有限的无限阿贝尔群．事实上，存在塔斯基（Tarski）怪物：一切真子群的阶都是素数的无限群.

对于 $k[x]$-模 V^T 的构造有一个重要的特殊情形．如果 A 是元素在 k 中的 $n\times n$ 矩阵，定义 $T: k^n \to k^n$ 为 $T(v) = Av$（回忆 k^n 的元素是 $n\times 1$ 列向量 v，从而 Av 是矩阵乘法）．我们记 $K[x]$-模$(k^n)^T$ 为 $(k^n)^A$ ；于是，$(k^n)^A$ 上的作用由

$$f(x)v = \left(\sum_{i=0}^{m} c_i x^i\right)v = \sum_{i=0}^{m} c_i A^i v$$

给出．

我们现在把上一节关于一般 PID 上模的结果应用到 $k[x]$-模 V^T 和 $(k^n)^A$ 上．如果 $T: V\to V$ 是线性变换，则 V^T 的子模 W 是**不变子空间**；即 V 的子空间 W 满足 $T(W)\subseteq W$，从而限制 $T\mid W$ 是 W 上的线性变换；即 $T\mid W: W\to W$.

定义 如果 A 是 $r\times r$ 矩阵和 B 是 $s\times s$ 矩阵，则它们的**直和** $A\oplus B$ 是指 $(r+s)\times(r+s)$ 矩阵

$$A\oplus B = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}.$$

引理 9.31 如果 $V^T = W\oplus W'$，其中 W 和 W' 都是子模，则

$$_{B\cup B'}[T]_{B\cup B'} = {}_B[T\mid W]_B \oplus {}_{B'}[T\mid W']_{B'},$$

其中 $B = w_1,\cdots,w_r$ 是 W 的基，$B' = w'_1,\cdots,w'_s$ 是 W' 的基．

证明 因 W 和 W' 都是子模，有 $T(W)\subseteq W$ 和 $T(W')\subseteq W'$；即限制 $T\mid W$ 和 $T\mid W'$ 分别是 W 和 W' 上的线性变换．因 $V = W\oplus W'$，所以 $B\cup B'$ 是 V 的基．最后，$_{B\cup B'}[T]_{B\cup B'}$ 是引理陈述中的直和：$T(w_i)\in W$，从而它是 $w_1,\cdots,w_r$ 的线性组合，因此它不需要对应 w'_j 的非零坐标；同样，[667] $T(w'_j)\in W'$，因此对应 w_i 的坐标全是 0. ∎

研究置换的时候，可以看到轮换记号使我们认识许多重要性质，而这些性质被习惯的函数记号所笼罩．我们现在问是否存在一种类似的方法来表示矩阵；精确地说，如果 V^T 是循环 $k[x]$-模，那么能够找到 V 的一组基 B 使得对应的矩阵呈现出 T 的重要性质吗？

引理 9.32 V^T 的子模 W 是有限阶的循环模当且仅当存在向量 $v\in W$ 和整数 $s\geqslant 1$ 使得

$$v, Tv, T^2v, \cdots, T^{s-1}v$$

是 W 的基．此外，如果

$$T^s v + \sum_{i=0}^{s-1} c_i T^i v = 0,$$

则阶理想 $\operatorname{ann}(v) = (g)$，其中 $g(x) = x^s + c_{s-1}x^{s-1} + \cdots + c_1 x + c_0$；即

$$W \cong k[x]/(g).$$

证明 假定 $W = \langle v\rangle = \{f(x)v: f(x)\in k[x]\}$．因 V，从而 W 是有限维向量空间，存在整数 $s\geqslant 1$ 和线性无关表 $v, Tv, T^2v, \cdots, T^{s-1}v$，而且再加一个 $T^s v$ 该表就线性相关．因此，存在 $c_i\in k$ 使得

$$T^s v + \sum_{i=0}^{s-1} c_i T^i v = 0.$$

如果 $w\in W$，则有某个 $f(x)\in k[x]$ 使得 $w = f(x)v$．对 $\deg(f)$ 容易用归纳法证明 w 在 $v, Tv, T^2v, \cdots, T^{s-1}v$ 张成的子空间中；由此这个表是 W 的基．

为证明逆命题，假定存在向量 $v\in W$ 和整数 $s\geqslant 1$ 使得表 $v, Tv, T^2v, \cdots, T^{s-1}v$ 是 W 的基．显然，$W\subseteq\langle v\rangle$，即由 v 生成的循环子模．反包含是明显的，这是因为我们假定 W 是子模；因此对每个 $f(x)\in k[x]$，$f(x)v\in W$．

多项式 $g(x)$ 在阶理想 $\operatorname{ann}(v)$ 中．如果 $h(x)\in\operatorname{ann}(v)$，带余除法给出 $q(x)$ 和 $r(x)$ 使得

$h = gq + r$，其中 $r = 0$ 或 $\deg(r) < \deg(g) = s$．但 $r(x) \in \mathrm{ann}(v)$，从而 $r(x) = \sum_{j=0}^{t} c_j x^j$．因此 $\sum_{j=0}^{t} c_j T^j v = 0$，其中 $t \leqslant s-1$，这与基的线性无关性矛盾．由此，$g(x)$ 是 $\mathrm{ann}(v)$ 中的一切多项式中次数最小的一个，从而 $\mathrm{ann}(v) = (g)$．所以 $W \cong k[x]/\mathrm{ann}(v) = k[x]/(g)$． ■

定义 如果 $g(x) = x + c_0$，则它的**友矩阵** $C(g)$ 是指 1×1 矩阵 $[-c_0]$；如果 $s \geqslant 2$ 和 $g(x) = x^s + c_{s-1}x^{s-1} + \cdots + c_1 x + c_0$，则它的**友矩阵** $C(g)$ 是 $s\times s$ 矩阵

668

$$\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & 0 & \cdots & 0 & -c_2 \\ 0 & 0 & 1 & \cdots & 0 & -c_3 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -c_{s-1} \end{bmatrix}$$

显然，可以从友矩阵 $C(g)$ 的最后一列得到多项式 $g(x)$．

引理 9.33 设 $T: V \to V$ 是域 k 上的向量空间 V 上的线性变换，且 V^T 是生成元为 v 的循环 $k[x]$-模．如果阶理想 $\mathrm{ann}(v) = (g)$，其中 $g(x) = x^s + c_{s-1}x^{s-1} + \cdots + c_1 x + c_0$，则 $B = v, Tv, T^2 v, \cdots, T^{s-1} v$ 是 V 的基，且矩阵 ${}_B[T]_B$ 是友矩阵 $C(g)$．

证明 设 $A = {}_B[T]_B$．根据定义，A 的第一列由 $T(v)$ 的坐标组成，第二列由 $T(Tv) = T^2 v$ 的坐标组成，并且一般来讲，如果 $i < s-1$，则 $T(T^i v) = T^{i+1} v$；即 T 把每个基向量送到下一个．然而，对于最后一个基向量，$T(T^{s-1}v) = T^s v$．但 $T^s v = -\sum_{i=0}^{s-1} c_i T^i v$，其中 $g(x) = x^s + \sum_{i=0}^{s-1} c_i x^i$．由此，${}_B[T]_B$ 是友矩阵 $C(g)$． ■

定理 9.34 （i）设 A 是元素在域 k 中的 $n\times n$ 矩阵．如果

$$(k^n)^A = W_1 \oplus \cdots \oplus W_r,$$

其中每个 W_i 都是循环的，比如有阶理想 (f_i)，则 A 相似于友矩阵的直和

$$C(f_1) \oplus \cdots \oplus C(f_r).$$

（ii）域 k 上的每个 $n\times n$ 矩阵 A 相似于友矩阵的直和

$$C(g_1) \oplus \cdots \oplus C(g_t),$$

其中 $g_i(x)$ 是首一多项式且

$$g_1(x) \mid g_2(x) \mid \cdots \mid g_t(x).$$

证明 定义 $V = k^n$，并定义 $T: V \to V$ 为 $T(y) = Ay$，其中 y 是列向量．

（i）根据引理 9.33，每个 W_i 有基 $B_i = v_i, Tv_i, T^2 v_i, \cdots$，且关于这组基 B_i，限制 $T \mid W_i$ 有矩阵 $C(f_i)$，它是 $f_i(x)$ 的友矩阵．关于基 $B_1 \cup \cdots \cup B_r$，根据命题 9.31，线性变换 T 有所要的矩阵．最后，根据系 3.101，A 相似于 $C(f_1) \oplus \cdots \oplus C(f_r)$．

669

（ii）根据例 9.30，有限生成 $k[x]$-模 V^T 是挠模，从而基定理，即命题 9.18 给出

$$(k^n)^A = W_1 \oplus W_2 \oplus \cdots \oplus W_t,$$

其中每个 W_i 是循环的，比如它的生成元 v_i 有阶理想 (g_i)，且 $g_1(x) \mid g_2(x) \mid \cdots \mid g_t(x)$．再由（i）

可得该命题． ■

定义 称矩阵 R 是**有理**[㊀]**典范**[㊁]**型**，如果它是友矩阵的直和，

$$R = C(g_1) \oplus \cdots \oplus C(g_t),$$

其中 $g_i(x)$ 是首一多项式，且 $g_1(x) \mid g_2(x) \mid \cdots \mid g_t(x)$．

如果矩阵 A 相似于有理典范型

$$C(g_1) \oplus \cdots \oplus C(g_t),$$

其中 $g_1(x) \mid g_2(x) \mid \cdots \mid g_t(x)$，则说 A 的**不变因子**是 $g_1(x), g_2(x), \cdots, g_t(x)$．

我们刚才证明了域 k 上的每个 $n \times n$ 矩阵相似于有理典范型，因此它有不变因子．一个矩阵 A 的不变因子表会不止一个吗？

定理 9.35 元素在域 k 中的两个 $n \times n$ 矩阵 A 和 B 相似当且仅当它们有相同的不变因子．此外，一个矩阵恰相似于一个有理典范型．

证明 根据系 3.101，A 和 B 相似当且仅当 $(k^n)^A \cong (k^n)^B$．根据定理 9.22，$(k^n)^A \cong (k^n)^B$ 当且仅当它们的不变因子相同．

对于给定的不变因子表 $g_1(x), g_2(x), \cdots, g_t(x)$ 只有一个有理典范型，就是 $C(g_1) \oplus \cdots \oplus C(g_t)$．如果一个矩阵相似于两个不同的有理典范型，则它有两个不同的不变因子表，与本定理的第一个陈述矛盾． ■

下面的定理类似于系 3.41，该系说明：如果 k 是域 K 的子域且 $f(x), g(x) \in k[x]$，则它们在 $k[x]$ 中的 gcd 等于它们在 $K[x]$ 中的 gcd.

670

系 9.36 （ⅰ）设 k 是域 K 的子域，并设 A 和 B 是元素在 k 中的 $n \times n$ 矩阵．如果 A 和 B 在 K 上相似，则它们在 k 上相似（即，如果存在元素在 K 中的非奇异矩阵 P 使得 $B = PAP^{-1}$，则存在元素在 k 中的非奇异矩阵 Q 使得 $B = QAQ^{-1}$）．

（ⅱ）如果 $\overline{k}$ 是域 k 的代数闭包，则元素在 k 中的两个 $n \times n$ 矩阵 A 和 B 在 k 上相似当且仅当它们在 $\overline{k}$ 上相似．

证明 （ⅰ）假设 $g_1(x), \cdots, g_t(x)$ 是把 A 看作 k 上矩阵的不变因子，而 $G_1(x), \cdots, G_q(x)$ 是把 A 看作 K 上矩阵的不变因子．根据定理，两个多项式表一致，这是因为 A 的两组不变因子都是把 A 看作 K 上的矩阵．

现在 B 和 A 在 K 上相似，所以它们有相同的不变因子；然而这些不变因子在 k 中，所以 A 和 B 在 k 上相似． ■

（ⅱ）由（ⅰ）立即可得．

例如，假设 A 和 B 都是实数矩阵，它们在复数上相似；即如果存在非奇异复数矩阵 P 使得 $B = PAP^{-1}$，则存在非奇异实数矩阵 Q 使得 $B = QAQ^{-1}$.

分析一个矩阵A的第一步是看它是否保持k^n的任一一维子空间不变；即有没有任一非零向量

㊀ 如果 $E \subseteq \mathbb{R}$ 是 $\mathbb{Q}$ 的扩张，则每个不在 $\mathbb{Q}$ 中的元素 $e \in E$ 是无理数．一般地，如果 E/k 是域扩张，则称底下的域 k 的元素为有理的．这里是在有理典范型（rational canonical form）中使用形容词有理（rational）的缘由，因为一个有理典范型的一切元素都在域 k 中，而不在它的某个扩张中．与之相比较，下一节讨论的若尔当典范型涉及矩阵的特征值，它可能不在 k 中．

㊁ 形容词典范（canonical）原来的意思是指宗教的某个教规，例如 canonical hours 是指进行祷告的时刻．扩大后的意思是指美好的事物，到了数学中是指由一般法则或公式给出的结果．

x 对某个标量 α 满足 $Ax=\alpha x$？我们称 α 为 A 的一个**特征值**，称 x 为 A 关于 α 的一个**特征向量**. 说非零 x 满足 $Ax=\alpha x$ 就是说 x 是齐次方程组 $(A-\alpha I)x=0$ 的非平凡解；即 $A-\alpha I$ 是奇异矩阵. 但元素在一个域中的矩阵是奇异的当且仅当它的行列式为 0. 回忆 A 的**特征多项式**是 $\psi_A(x)=\det(xI-A)\in k[x]$[⊖]，因此 A 的特征值是 $\psi_A(x)$ 的根. 如果 $\overline{k}$ 是 k 的代数闭包，则 $\psi_A(x)=\prod_{i=1}^{n}(x-\alpha_i)$，因此 $\psi_A(x)$ 的常数项是 $(-1)^n\prod\alpha_i$. 另一方面，任一多项式 $f(x)$ 的常数项正是 $f(0)$；在 $\psi_A(x)=\det(xI-A)$ 中令 $x=0$ 得 $\psi_A(0)=(-1)^n\det(A)$. 由此，$\det(A)$ 是特征值的积

下面是关于特征值的一些基本事实.

系 9.37 设 A 是元素在域 k 中的 $n\times n$ 矩阵.

(i) A 是奇异的当且仅当 0 是 A 的一个特征值.

(ii) 如果 α 是 A 的一个特征值，则 α^n 是 A^n 的一个特征值.

(iii) 如果 A 是非奇异的且 α 是 A 的一个特征值，则 $\alpha\neq 0$ 且 α^{-1} 是 A^{-1} 的一个特征值. [671]

证明 (i) 如果 A 是奇异的，则齐次方程组 $Ax=0$ 有非平凡解；即存在非零向量 x 满足 $Ax=0$. 但这就是说 $Ax=0x$，因此 0 是一个特征值.

反之，如果 0 是一个特征值，则 $0=\det(0I-A)=\pm\det(A)$，因此 $\det(A)=0$，A 是奇异的.

(ii) 存在非零向量 v 满足 $Av=\alpha v$. 对 $n\geqslant 1$ 用归纳法可证明 $A^n v=\alpha^n v$.

(iii) 如果 x 是 A 和 α 的特征向量，则

$$x=A^{-1}Ax=A^{-1}\alpha x=\alpha A^{-1}x.$$

所以，$\alpha\neq 0$（因为特征向量非零）和 $\alpha^{-1}x=A^{-1}x$. ■

回到典范型.

定理 9.38 如果 $g(x)\in k[x]$，则 $\det(xI-C(g))=g(x)$.

证明 如果 $\deg(g)=s\geqslant 2$，则

$$xI-C(g)=\begin{bmatrix} x & 0 & 0 & \cdots & 0 & c_0 \\ -1 & x & 0 & \cdots & 0 & c_1 \\ 0 & -1 & x & \cdots & 0 & c_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -1 & x+c_{s-1} \end{bmatrix}.$$

对第一行用拉普拉斯展开式得

$$\det(xI-C(g))=x\det(L)+(-1)^{1+s}c_0\det(M),$$

其中 L 是删去第一行和第一列得到的矩阵，M 是由删去第一行和最后一列得到的矩阵. 现在 M 是 $(s-1)\times(s-1)$ 三角矩阵，对角线上元素是 -1，而 $L=xI-C((g(x)-c_0)/x)$. 根据归纳假设，$\det(L)=(g(x)-c_0)/x$，而 $\det(M)=(-1)^{s-1}$. 所以，

$$\det(xI-C(g))=x[(g(x)-c_0)/x]+(-1)^{(1+s)+(s-1)}c_0=g(x).$$ ■

如果 $R=C(g_1)\oplus\cdots\oplus C(g_t)$ 是有理典范型，则

$$xI-R=[xI-C(g_1)]\oplus\cdots\oplus[xI-C(g_t)],$$

⊖ 我们继续沿用行列式的熟知性质，即使这些性质要到 9.9 节才证明.

引理和命题 9.163 说 $\det(B_1 \oplus \cdots \oplus B_t) = \prod_i \det(B_i)$，因此得

$$\psi_R(x) = \prod_{i=1}^{t} \psi_{C(g_i)}(x) = \prod_{i=1}^{t} g_i(x).$$

于是，特征多项式是不变因子的积；根据系 9.20，域 k 上的 $n\times n$ 矩阵 A 的特征多项式是 $(k^n)^A$ 的
672
类似于有限阿贝尔群的阶．

例 9.39 我们现在证明相似矩阵有相同的特征多项式．如果 $B=PAP^{-1}$，则因 xI 和每个矩阵都可交换，所以有 $P(xI)=(xI)P$，因此，$P(xI)P^{-1}=(xI)PP^{-1}=xI$．所以，

$$\begin{aligned}\psi_B(x) &= \det(xI-B)\\ &= \det(PxIP^{-1}-PAP^{-1})\\ &= \det(P[xI-A]P^{-1})\\ &= \det(P)\det(xI-A)\det(P^{-1})\\ &= \det(xI-A)\\ &= \psi_A(x).\end{aligned}$$

由此，如果 A 相似于 $C(g_1)\oplus\cdots\oplus C(g_t)$，则

$$\psi_A(x) = \prod_{i=1}^{t} g_i(x).$$

所以，相似矩阵有相同的特征值连同其重数. ■

定理 9.40（凯莱-哈密顿） 如果 A 是有特征多项式 $\psi_A(x)=x^n+b_{n-1}x^{n-1}+\cdots+b_1x+b_0$ 的 $n\times n$ 矩阵，则 $\psi_A(A)=0$；即

$$A^n+b_{n-1}A^{n-1}+\cdots+b_1A+b_0I=0.$$

证明 根据例 9.39，可以假定 $A=C(g_1)\oplus\cdots\oplus C(g_t)$ 是有理典范型，其中 $\psi_A(x)=g_1(x)\cdots g_t(x)$．如果把 k^n 看作 $k[x]$-模 $(k^n)^A$，则系 9.19 说对一切 $y\in k^n$，$g_t(A)y=0$．于是，$g_t(A)=0$．然而，因 $g_t(x)\mid\psi_A(x)$，所以有 $\psi_A(A)=0$． ■

凯莱-哈密顿定理和系 2.44 类似．

定义 一个 $n\times n$ 矩阵 A 的**最小多项式** $m_A(x)$ 是指具有性质 $f(A)=0$ 的次数最小的首一多项式 $f(x)$．

命题 9.41 最小多项式 $m_A(x)$ 是特征多项式 $\psi_A(x)$ 的因式，且 A 的每个特征值都是 $m_A(x)$ 的根.

证明 凯莱-哈密顿定理证明 $m_A(x)\mid\psi_A(x)$，而系 9.19 蕴涵 $c_t(x)$ 是 A 的最小多项式，其中 $c_t(x)$ 是 A 的次数最高的不变因子．由此，从事实

$$\psi_A(x)=c_1(x)\cdots c_t(x)$$

(其中 $c_1(x)\mid c_2(x)\mid\cdots\mid c_t(x)$) 可知 $m_A(x)=c_t(x)$ 是最小多项式，且以 A 的每个特征值为根[当
673
然，作为 $m_A(x)$的一个根，它的重数可能小于作为特征多项式 $\psi_A(x)$ 的根的重数]. ■

系 9.42 如果 $n\times n$ 矩阵 A 的一切特征值都不同，则 $m_A(x)=\psi_A(x)$；即最小多项式和特征多项式一致．

证明 因为 $\psi_A(x)$ 的每个根都是 $m_A(x)$ 的根，所以命题成立. ■

系 9.43 （i）$n\times n$ 矩阵 A 相似于一个友矩阵当且仅当

$$m_A(x)=\psi_A(x).$$

（ii）有限阿贝尔群 G 是循环的当且仅当它的指数等于它的阶．

证明 （i）友矩阵 $C(g)$ 只有一个不变因子，就是 $g(x)$；但系 9.19 把最小多项式等同于最后

一个不变因子．

如果 $m_A(x)=\psi_A(x)$，则根据系 9.20，A 只有一个不变因子，就是 $\psi_A(x)$．因此，A 和 $C(\psi_A(x))$ 有相同的不变因子，所以它们相似．

（ⅱ）n 阶循环群只有一个不变因子，就是 n；但系 9.19 把指数等同于最后一个不变因子．

如果 G 的指数等于它的阶 $|G|$，则 G 只有一个不变因子，就是 $|G|$．因此 G 和 $\mathbb{I}_{|G|}$ 有相同的不变因子，从而它们同构．■

习题

9.32 （ⅰ）$\mathbb{R}$ 上满足 $A^2=I$ 的 10×10 矩阵（如不计相似）有多少？

（ⅱ）$\mathbb{F}_p$ 上满足 $A^2=I$ 的 10×10 矩阵（如不计相似）有多少？

提示：答案依赖于 p 是奇数还是 $p=2$.

9.33 求下列矩阵的有理典范型：

$$A=\begin{bmatrix}1&2\\3&4\end{bmatrix},B=\begin{bmatrix}2&0&0\\1&2&0\\0&0&3\end{bmatrix}\text{和 }C=\begin{bmatrix}2&0&0\\1&2&0\\0&1&2\end{bmatrix}.$$

9.34 如果 A 相似于 A'，B 相似于 B'，证明 $A\oplus B$ 相似于 $A'\oplus B'$.

9.35 设 k 是域，并设 $f(x)$ 和 $g(x)$ 在 $k[x]$ 中．如果 $g(x)\mid f(x)$ 且 $f(x)$ 的每个根都是 $g(x)$ 的根，证明存在矩阵 A，它有极小多项式 $m_A(x)=g(x)$ 和特征多项式 $\psi_A(x)=f(x)$．

9.36 （ⅰ）举出两个不同构有限阿贝尔群的例子，它们的阶和指数都相同.

（ⅱ）举出两个不相似矩阵的例子，它们的特征多项式和最小多项式都相同．

674

9.3 若尔当典范型

如果 k 是有限域，则 $\mathrm{GL}(n,k)$ 是有限群，从而其中的每个元素的阶有限．考虑群论问题：A 在 $\mathrm{GL}(3,\mathbb{F}_7)$ 中的阶是多少，其中

$$A=\begin{bmatrix}0&0&1\\1&0&4\\0&1&3\end{bmatrix}?$$

当然，可以计算幂 A^2，A^3，…；拉格朗日定理保证有某个 $n\geqslant1$ 使得 $A^n=E$，但用这个方法求 A 的阶十分麻烦．我们可以把 A 认作

$$g(x)=x^3-3x^2-4x-1=x^3-3x^2+3x-1=(x-1)^3$$

的友矩阵（记住 $g(x)\in\mathbb{F}_7[x]$）．现在 A 和 PAP^{-1} 在群 $\mathrm{GL}(n,k)$ 中共轭，因此它们有相同的阶．但友矩阵的幂很复杂（例如，一个友矩阵的平方就不是一个友矩阵）．我们现在给出容易计算其幂的第二种典范型，本节后面将用它来计算 A 的阶.

定义 一个 1×1 **若尔当块**是指矩阵 $J(\alpha,1)=[\alpha]$．如果 $s\geqslant2$，则 $s\times s$ **若尔当块**是指形如

$$J(\alpha,s)=\begin{bmatrix}\alpha&0&0&\cdots&0&0\\1&\alpha&0&\cdots&0&0\\0&1&\alpha&\cdots&0&0\\\vdots&\vdots&\vdots&\vdots&\vdots&\vdots\\0&0&0&\cdots&\alpha&0\\0&0&0&\cdots&1&\alpha\end{bmatrix}$$

的矩阵 $J(\alpha,s)$.

这里是若尔当块的更简洁的描述. 令 L 表示除了主对角线下面的次对角线的元素为 1 之外其他元素都是 0 的 $s\times s$ 矩阵. 用这个记号，一个若尔当块 $J(\alpha,s)$ 形如

$$J(\alpha,s)=\alpha I+L.$$

我们把 L 看作 k^s 上的线性变换. 如果 $e_1,\cdots,e_s$ 是标准基，则对 $t<s, Le_i=e_{i+1}$ 而 $Le_s=0$. 易知矩阵 L^2 是主对角线下面的第二次对角线的元素为 1，其他元素都是 0；L^3 是第三次对角线的元素为 1 而其他元素都是 0；L^{s-1} 在 s 和 1 的位置是 1 而其他都是 0，以及 $L^s=0$.

675

定理 9.44 如果 $J=J(\alpha,s)=\alpha I+L$ 是 $s\times s$ 若尔当块，则对一切 $m\geqslant 1$，

$$J^m=\alpha^m I+\sum_{i=1}^{s-1}\binom{m}{i}\alpha^{m-i}L^i.$$

证明 因 L 和 αI 可交换（事实上，αI 和每个矩阵都可交换），αI 的幂和 L 的幂的线性组合的全体是一个（交换）环，因此二项式定理适用. 最后，因为 $L^s=0$，对 $i\geqslant s$，所有涉及 L^i 的项是 0. ■

例 9.45 L 的不同幂"不相交"：即如果 $m\neq n$ 且 L^n 的 ij 元素非零，则 L^m 的 ij 元素为零：

$$\begin{bmatrix}\alpha & 0\\ 1 & \alpha\end{bmatrix}^m=\begin{bmatrix}\alpha^m & 0\\ m\alpha^{m-1} & \alpha^m\end{bmatrix}$$

和

$$\begin{bmatrix}\alpha & 0 & 0\\ 1 & \alpha & 0\\ 0 & 1 & \alpha\end{bmatrix}^m=\begin{bmatrix}\alpha^m & 0 & 0\\ m\alpha^{m-1} & \alpha^m & 0\\ \binom{m}{2}\alpha^{m-2} & m\alpha^{m-1} & \alpha^m\end{bmatrix}.$$ ■

定理 9.46 如果 $g(x)=(x-\alpha)^s$，则友矩阵 $C(g)$ 相似于 $s\times s$ 若尔当块 $J(\alpha,s)$.

证明 如果 $T: k^s\to k^s$ 定义为 $z\mapsto C(g)z$，则定理 9.33 的证明给出 k^s 的基形如 $v, Tv, T^2v,\cdots, T^{s-1}v$. 我们断言表 $Y=y_0,\cdots,y_{s-1}$ 也是 k^s 的基，其中

$$y_0=v, y_1=(T-\alpha I)v,\cdots,y_{s-1}=(T-\alpha I)^{s-1}v.$$

易知表 Y 张成 V，这是因为对一切 $0\leqslant i\leqslant s-1, T^iv\in\langle y_0,\cdots,y_i\rangle$. 因 Y 中有 s 个元素，命题 3.87 证明 Y 是基.

我们现在计算 $J={}_Y[T]_Y$. 如果 $j+1\leqslant s$，则

$$\begin{aligned}Ty_j&=T(T-\alpha I)^jv\\&=(T-\alpha I)^jTv\\&=(T-\alpha I)^j[\alpha I+(T-\alpha I)]v\\&=\alpha(T-\alpha I)^jv+(T-\alpha I)^{j+1}v.\end{aligned}$$

因此，如果 $j+1<s$，则

$$Ty_j=\alpha y_j+y_{j+1}.$$

如果 $j+1=s$，则根据凯莱-哈密顿定理 [对 $\psi_{C(g)}(x)=(x-\alpha)^s$]，

$$(T-\alpha I)^{j+1}v=(T-\alpha I)^sv=0,$$

676

因此 $Ty_{s-1}=\alpha y_{s-1}$. 于是矩阵 J 是若尔当块 $J(\alpha,s)$. 根据系 3.101，$C(g)$ 和 $J(\alpha,s)$ 相似. ■

由此，正如友矩阵一样，若尔当块也对应多项式，特别地，$J(\alpha,s)$ 对应 $(x-\alpha)^s$.

定理 9.47 设 A 是元素在域 k 中的 $n\times n$ 矩阵. 如果 k 包含 A 的一切特征值（特别地，如果 k 是代数闭的），则 A 相似于若尔当块的一个直和.

证明 我们现在不用不变因子 $g_1 \mid g_2 \mid \cdots \mid g_t$，而用基定理中出现的初等因子 $f_i(x)$；即每个 $f_i(x)$ 都是 $k[x]$ 中不可约多项式的积. 根据定理 9.34(ⅰ)，把$(k^n)^A$ 分解为循环 $k[x]$-模 W_i 的直和产生友矩阵的直和

$$U = C(f_1) \oplus \cdots \oplus C(f_r),$$

其中 (f_i) 是 W_i 的阶理想，且 U 和 A 相似. 然而，因 $\psi_A(x) = \prod_i f_i(x)$，我们的假设说每个 $f_i(x)$ 在 k 上分裂；即有某个 $s_i \geqslant 1$ 使得 $f_i(x) = (x-\alpha_i)^{s_i}$，其中 α_i 是 A 的特征值. 根据引理，$C(f_i)$ 相似于若尔当块，根据习题 9.34，A 相似于若尔当块的直和. ■

定义 **若尔当典范型**是若尔当块的直和.

如果矩阵 A 相似于若尔当典范型

$$J(\alpha_1, s_1) \oplus \cdots \oplus J(\alpha_r, s_r),$$

则说 A 有**初等因子** $(x-\alpha_1)^{s_1}, \cdots, (x-\alpha_r)^{s_r}$.

定理 9.47 说元素在包含 A 的一切特征值的域中的方矩阵 A 相似于一个若尔当典范型. 一个矩阵能够相似于几个若尔当典范型吗？回答是，但不确切.

例 9.48 设 I_r 是 $r\times r$ 单位矩阵，并设 I_s 是 $s\times s$ 单位矩阵，则在直和中交换它的块产生一个相似矩阵：

$$\begin{bmatrix} B & 0 \\ 0 & A \end{bmatrix} = \begin{bmatrix} 0 & I_r \\ I_s & 0 \end{bmatrix} \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix} \begin{bmatrix} 0 & I_s \\ I_r & 0 \end{bmatrix}.$$

因每个置换都是对换的积，所以对形如 $A_1 \oplus A_2 \oplus \cdots \oplus A_t$ 的矩阵中的块进行置换产生和它相似的矩阵. ■

定理 9.49 如果 A 和 B 都是域 k 上的 $n\times n$ 矩阵，其中 k 包含它们的一切特征值，则 A 和 B 相似当且仅当它们有相同的初等因子. 此外，一个矩阵 A 相似于两个若尔当典范型，比如 H 和 H'，则 H 和 H' 有相同的若尔当块.（即置换 H 中的若尔当块得 H'）.

677

证明 根据系 3.101，A 和 B 相似当且仅当 $(k^n)^A \cong (k^n)^B$. 根据定理 9.22，$(k^n)^A \cong (k^n)^B$ 当且仅当它们的初等因子相同.

不变因子是用特定的顺序给出的（每一个整除下一个），与之相比，一个行列式只是初等因子的集合，因此只是若尔当块的集合. 根据例 9.48，在给定的若尔当典范型中置换它的若尔当块得到的不同的若尔当典范型都相似. ■

下面是若尔当典范型的一些应用.

命题 9.50 如果 A 是元素在域 k 中的 $n\times n$ 矩阵，则 A 和它的转置 A^t 相似.

证明 首先，系9.36(ⅱ)允许我们假定 k 包含 A 的一切特征值. 现在如果 $B = PAP^{-1}$，则 $B^t = (P^t)^{-1}A^tP^t$；即如果 B 和 A 相似，则 B^t 和 A^t 相似. 于是只要证明若尔当典范型 H 相似于 H^t，并且根据习题 9.34，只要证明若尔当块 $J = J(\alpha, s)$ 相似于 J^t 就够了.

我们用 $J(\alpha,3)$ 说明. 设 Q 是“反”对角线元素为 1 而其他元素都是 0 的矩阵，注意 $Q = Q^{-1}$.

$$\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} \alpha & 0 & 0 \\ 1 & \alpha & 0 \\ 0 & 1 & \alpha \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} \alpha & 1 & 0 \\ 0 & \alpha & 1 \\ 0 & 0 & \alpha \end{bmatrix}$$

我们让读者证明，一般来说有 $Q=Q^{-1}$ 和 $QJ(\alpha,s)Q^{-1}=J(\alpha,s)^t$．或许最有效的证明是设 v_1，…，v_s 为向量空间 W 的基，定义 $Q: W\to W$ 为 $Q: v_i\mapsto v_{s-i+1}$，并定义 $J: W\to W$ 为 $J: v_i\mapsto \alpha v_i+v_{i+1}$（其中 $i<s$）和 $J: v_s\mapsto \alpha v_s$. ■

例 9.51 本节开始时，我们要求矩阵 A 在 $\mathrm{GL}(3,\mathbb{F}_7)$ 中的阶，其中

$$A=\begin{bmatrix}0&0&1\\1&0&4\\0&1&3\end{bmatrix};$$

可以看到 A 是 $(x-1)^3$ 的友矩阵．因 $\psi_A(x)$ 是 $x-1$ 的幂，A 的特征值全都等于 1，因此在$\mathbb{F}_7$ 中；根据引理 9.46，A 相似于若尔当块

$$J=\begin{bmatrix}1&0&0\\1&1&0\\0&1&1\end{bmatrix}.$$

根据例 9.45，

$$J^m=\begin{bmatrix}1&0&0\\m&1&0\\\binom{m}{2}&m&1\end{bmatrix},$$

678

因为在$\mathbb{F}_7$ 中有 $7=0$ 和 $\binom{7}{2}=21=0$，所以 $J^7=I$．因此 A 在 $\mathrm{GL}(3,\mathbb{F}_7)$中的阶为 7. ■

线性微分方程组可以通过对矩阵取幂来求解；对矩阵取幂在建立一个李群和它对应的李代数之间的关系时也十分有用．一个 $n\times n$ 复数矩阵 A 由 n^2 个元素组成，从而可以把 A 看作$\mathbb{C}^{n^2}$ 中的一个点．这就可以定义 $n\times n$ 复数矩阵序列的收敛性：称 A_1，A_2，…，A_k，…**收敛**到矩阵 M，如果对每对 i，j，位于 i，j 的元素的序列收敛．和微积分中的定义一样，一个级数收敛是指它的部分和序列收敛．

定义 如果 A 是一个 $n\times n$ 复数矩阵，则

$$e^A=\sum_{k=0}^{\infty}\frac{1}{k!}A^k=I+A+\frac{1}{2}A^2+\frac{1}{6}A^3+\cdots.$$

可以证明这个级数对每个矩阵 A 都收敛，且函数 $A\mapsto e^A$ 是连续的；即如果 $\lim\limits_{k\to\infty}A_k=M$，则

$$\lim_{k\to\infty}e^{A_k}=e^M.$$

下面是这个矩阵幂的一些性质；我们将看到若尔当典范型使我们能够计算 e^A.

命题 9.52 设 A 是 $n\times n$ 复数矩阵.

(i) 如果 P 是非奇异矩阵，则 $Pe^AP^{-1}=e^{PAP^{-1}}$.

(ii) 如果 $AB=BA$，则 $e^Ae^B=e^{A+B}$.

(iii) 对每个矩阵 A，矩阵 e^A 是非奇异的，事实上，

$$(e^A)^{-1}=e^{-A}.$$

(iv) 如果 L 是紧接主对角线之下的元素是 1 而其他元素都是 0 的 $n\times n$ 矩阵，则 e^L 是对角线元素为 1 的下三角矩阵.

(v) 如果 D 是对角矩阵，比如 $D=\mathrm{diag}(\alpha_1,\alpha_2,\cdots,\alpha_n)$，则

$$e^D=\mathrm{diag}(e^{\alpha_1},e^{\alpha_2},\cdots,e^{\alpha_n}).$$

(vi) 如果 α_1, α_2, …, α_n 是 A 的特征值（具有重数），则 e^{α_1}, …, e^{α_n} 是 e^A 的特征值.

(vii) 能够计算 e^A.

(viii) 如果 $\operatorname{tr}(A)=0$，则 $\det(e^A)=1$.

679

证明 (i) 我们用矩阵幂的连续性.

$$\begin{aligned}Pe^AP^{-1} &= P\Big(\lim_{n\to\infty}\sum_{k=0}^{n}\frac{1}{k!}A^k\Big)P^{-1}\\&=\lim_{n\to\infty}\sum_{k=0}^{n}\frac{1}{k!}(PA^kP^{-1})\\&=\lim_{n\to\infty}\sum_{k=0}^{n}\frac{1}{k!}(PAP^{-1})^k\\&=e^{PAP^{-1}}.\end{aligned}$$

(ii) e^{A+B}的幂级数的第 k 项的系数是

$$\frac{1}{k!}(A+B)^k,$$

而 e^Ae^B 的第 k 项是

$$\sum_{i+j=k}\frac{1}{i!}A^i\frac{1}{j!}B^j=\sum_{i=0}^{k}\frac{1}{i!(k-i)!}A^iB^{k-i}=\frac{1}{k!}\sum_{i=0}^{k}\binom{k}{i}A^iB^{k-i}.$$

因 A 和 B 可交换，二项式定理表明两个第 k 项的系数相等. 如果 A 和 B 不可交换，则结论不成立，见习题 9.44.

(iii) 由 (ii) 立即可得，这是因为 $-A$ 和 A 可交换和 $e^0=I$.

(iv) 因为 $L^s=0$，等式

$$e^L=I+L+\frac{1}{2}L^2+\cdots+\frac{1}{(s-1)!}L^{s-1}$$

成立，由引理 9.44 可得结果. 例如，当 $s=5$ 时，

$$e^L=\begin{bmatrix}1&0&0&0&0\\1&1&0&0&0\\\frac{1}{2}&1&1&0&0\\\frac{1}{6}&\frac{1}{2}&1&1&0\\\frac{1}{24}&\frac{1}{6}&\frac{1}{2}&1&1\end{bmatrix}.$$

(v) 由定义

$$e^D=I+D+\frac{1}{2}D^2+\frac{1}{6}D^3+\cdots,$$

680

因

$$D^k=\operatorname{diag}(\alpha_1^k,\alpha_2^k,\cdots,\alpha_n^k),$$

结果显然成立.

(vi) 因C是代数闭域，A 相似于它的若尔当典范型 J：存在非奇异矩阵 P 使得 $PAP^{-1}=J$. 现在A 和 J有相同的特征多项式，因此有相同的有重数的特征值. 但 J 是下三角矩阵，对角线元素是

A 的特征值 $\alpha_1,\cdots,\alpha_n$，由此，矩阵幂的定义给出 e^J 是下三角矩阵，对角线元素是 $e^{\alpha_1},\cdots,e^{\alpha_n}$. 因 $e^A=e^{P^{-1}JP}=P^{-1}e^JP$，从而 e^A 的特征值如所断言的那样.

（vii）根据习题 9.38，存在非奇异矩阵 P 使得 $PAP^{-1}=\Delta+L$，其中 Δ 是对角矩阵，$L^n=0$，$\Delta L=L\Delta$. 因此，

$$Pe^AP^{-1}=e^{PAP^{-1}}=e^{\Delta+L}=e^{\Delta}e^L.$$

但（v）计算出 e^{Δ}，（iv）计算出 e^L. 因此，$e^A=P^{-1}e^{\Delta}e^LP$ 是可以计算的.

（viii）根据定义，矩阵的迹是特征值的和，而矩阵的行列式是特征值的积. 因 e^A 的特征值是 $e^{\alpha_1},\cdots,e^{\alpha_n}$，所以有

$$\det(e^A)=\prod_i e^{\alpha_i}=e^{\sum_i \alpha_i}=e^{\mathrm{tr}(A)}.$$

因此，$\mathrm{tr}(A)=0$ 蕴涵 $\det(e^A)=1$. ■

习题

9.37 求域 k 上满足 A 和 A^2 相似的一切 $n\times n$ 矩阵.

9.38 （**若尔当分解**）证明代数闭域 k 上的每个 $n\times n$ 矩阵 A 都能写成

$$A=D+N,$$

其中 D 是可对角化的（即 D 相似于一个对角矩阵），N 是幂零的（即有某个 $m\geqslant 1$ 使得 $N^m=0$），且 $DN=ND$.

注：如果 k 是完满域，则矩阵的若尔当分解是唯一的.

9.39 举出一个不可对角化的 $n\times n$ 矩阵的例子.

提示：已知每个实对称矩阵都是可对角化的. 反之，$\mathbb{R}^2$ 上绕原点（不是恒等的）的旋转不能把过原点的直线发送到它自己.

9.40 （i）证明幂零矩阵的一切特征值都是 0.

（ii）用若尔当型证明逆命题：如果矩阵 A 的一切特征值都是 0，则 A 是幂零的.（这个结果也来自凯莱-哈密顿定理.）

9.41 6×6 幂零实矩阵有多少相似类？

681

9.42 如果 A 是非奇异矩阵，且 A 相似于 B，证明 A^{-1} 和 B^{-1} 相似.

9.43 （i）证明每个幂零矩阵 N 和一个严格下三角矩阵（即对角线及对角线以上元素都是 0）相似.

（ii）如果 N 是幂零矩阵，证明 $I+N$ 是非奇异的.

9.44 设

$$A=\begin{bmatrix}1&0\\0&0\end{bmatrix}\text{和 } B=\begin{bmatrix}0&1\\0&0\end{bmatrix},$$

证明 $e^Ae^B\neq e^Be^A$，并由此推出 $e^Ae^B\neq e^{A+B}$.

9.45 在 $\mathrm{GL}(3,\mathbb{F}_7)$ 中有多少个共轭类？

9.46 我们知道 $\mathrm{PSL}(3,\mathbb{F}_4)$ 是 $20\,160=\frac{1}{2}8!$ 阶单群. 现在 A_8 包含一个 15 阶元素，就是 $(1\ 2\ 3\ 4\ 5)(6\ 7\ 8)$. 证明 $\mathrm{PSL}(3,\mathbb{F}_4)$ 没有 15 阶元素，由此可知 $\mathrm{PSL}(3,\mathbb{F}_4)\not\cong A_8$.

提示：用系 9.36，把 $\mathbb{F}_4$ 换成包含一个矩阵的任意必需的特征值的大域. 计算可能的若尔当典范型

$$A=\begin{bmatrix}a&0&0\\1&a&0\\0&1&a\end{bmatrix},B=\begin{bmatrix}a&0&0\\0&b&0\\0&1&b\end{bmatrix}\text{和 } C=\begin{bmatrix}a&0&0\\0&b&0\\0&0&c\end{bmatrix}$$

的阶［在群 $\mathrm{PSL}(3,\mathbb{F}_4)$ 中］.

9.4 史密斯正规型

我们对典范型的讨论中有一个缺陷：如何求出一个给定矩阵的不变因子？下面进行的讨论将给出计算不变因子的算法．特别是计算了 A 的极小多项式.

在第 3 章中，我们证明，一旦 V 的基 Y 和 W 的基 Z 选定后，有限维向量空间之间的线性变换 $T:V\to W$ 便确定了一个矩阵，且命题 3.98 表明矩阵乘法来自两个线性变换的复合所确定的矩阵. 现在把这个计算推广到自由 R-模之间的 R-映射上，其中 R 是任意交换环.

定义 设 R 是交换环，并设 $T:R^t\to R^n$ 是 R-映射，其中 R^t 和 R^n 是秩分别为 t 和 n 的自由 R-模. 如果 $Y=y_1,\cdots,y_t$ 是 R^t 的基，$Z=z_1,\cdots,z_n$ 是 R^n 的基，则

$$_Z[T]_Y=[a_{ij}]$$

是 R 上的 $n\times t$ 矩阵，对一切 i，它的第 i 列由 $T(y_i)$ 的坐标组成；即

$$T(y_i)=\sum_{j=1}^{n}a_{ji}z_j.$$

我们现在比较一个 R-同态 T 在 R^t 和 R^n 的不同基下的矩阵. 下一命题把系 3.101 从向量空间推广到交换环上的模.

682

命题 9.53 设 R 是交换环，设 R^t 和 R^n 是秩分别为 t 和 n 的自由 R-模，并设 $T:R^t\to R^n$ 是R-同态. 令 Y 和 Y'是 R^t 的基，Z 和 Z'是 R^n 的基. 如果 $\Gamma={}_Z[T]_Y$ 和 $\Gamma'={}_{Z'}[T]_{Y'}$，则存在可逆矩阵 P 和 Q，其中 P 是 $t\times t$ 矩阵和 Q 是 $n\times n$ 矩阵，使得

$$\Gamma'=Q\Gamma P^{-1}.$$

反之，如果 Γ 和 Γ'是 R 上的 $n\times t$ 矩阵满足 $\Gamma'=Q\Gamma P^{-1}$，其中 P 和 Q 是某可逆矩阵，则存在R-同态 $T:R^t\to R^n$（R^t 的基是 Y 和 Y',R^n 的基是 Z 和 Z'）使得 $\Gamma={}_Z[T]_Y$ 和 $\Gamma'={}_{Z'}[T]_{Y'}$.

证明 和系 3.101 中所做的计算相同，应用公式

$$_Z[S]_{YY}[T]_X={}_Z[ST]_X,$$

其中 $T:V\to V'$ 和 $S:V'\to V''$，且 X，Y，Z 分别是 V，V'，V''的基. 注意，原来的证明并未用到矩阵元素的逆，从而早先的元素在一个域中的假设太强；它们可以在任意一个交换环中. ■

定义 称元素在交换环 R 中的两个 $n\times t$ 矩阵 Γ 和 Γ'**R-等价**，如果存在元素在 R 中的可逆矩阵 P 和 Q 使得

$$\Gamma'=Q\Gamma P$$

（写作 P 和写作 P^{-1}具有同样的一般性）.

当然，刚才定义的等价是 R 上的一切（长方）$n\times t$ 矩阵集合上的等价关系.

命题 9.54 如果 R 是交换环，则（有限表现的）R-模 M 和 M'的有限表现给出正合列

$$R^t\xrightarrow{\lambda}R^n\xrightarrow{\pi}M\to 0 \text{ 和 } R^{t'}\xrightarrow{\lambda'}R^{n'}\xrightarrow{\pi'}M'\to 0,$$

且选取 R^t 的基 Y，Y'和 R^n 的基 Z，Z'给出矩阵 $\Gamma={}_Z[\lambda]_Y$ 和 $\Gamma'={}_{Z'}[\lambda']_{Y'}$. 如果 $t'=t$，$n'=n$，且 Γ 和 Γ' R-等价，则 $M\cong M'$.

证明 因 Γ 和 Γ' R-等价，存在可逆矩阵 P 和 Q 使得 $\Gamma'=Q\Gamma P^{-1}$；现在 P 确定一个 R-同态 $\theta:R^n\to R^n$，Q 确定一个 R-同态 $\varphi:R^t\to R^t$. 等式 $\Gamma'=Q\Gamma P^{-1}$蕴涵下图交换：

$$\begin{array}{ccccccc} R^t & \xrightarrow{\lambda} & R^n & \xrightarrow{\pi} & M & \longrightarrow & 0 \\ \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle\theta} & & \downarrow{\scriptstyle\nu} & & \\ R^t & \xrightarrow{\lambda'} & R^n & \xrightarrow{\pi'} & M' & \longrightarrow & 0 \end{array}$$

683

定义 R-映射 $\nu: M \to M'$ 如下：如果 $m \in M$，则 π 的满射性给出元素 $u \in R^n$ 使得 $\pi(u) = m$；令 $\nu(m) = \pi'\theta(u)$．命题 8.93 用图上追踪法证明 ν 是合理定义的同构. ■

命题 9.54 实质上是无用的；对大多数交换环 R，没有方法能够确定元素在 R 中的矩阵 Γ 和 Γ' 是否 R-等价. 然而，当 R 是欧几里得环时，我们能够用命题中的准则求出矩阵的可计算的正规型.

如果 $T: V \to V$ 是域 k 上的向量空间 V 的线性变换，则下一定理给出 $k[x]$-模 V^T 的有限表现. 下一定义由域 k 上的任意向量空间 V 建立一个自由 $k[x]$-模；这个构造基于第 3 章中对 $k[x]$ 的形式定义，那里把 $k[x]$ 定义为几乎一切坐标为零的 k 中的序列.

定义 如果 V 是交换环 k 上的 k-模，定义

$$V[x] = \sum_{i \geqslant 0} V_i,$$

其中对一切 i，$V_i \cong V$. 更详细地说，把 V_i 的元素记为 $x^i v$，其中 $v \in V$（因此 x^i 仅仅注明了坐标的位置；特别地，令 $x^0 v = v$，从而 $V_0 = V$）. 于是，每个元素 $u \in V[x]$ 有形如

$$u = \sum_{i \geqslant 0} x^i v_i$$

的唯一表达式，其中 $v_i \in V$ 且几乎一切 $v_i = 0$. 如果定义

$$x\Big(\sum_i x^i v_i\Big) = \sum_i x^{i+1} v_i,$$

则 k-模 $V[x]$ 是 $k[x]$-模.

对习惯张量积的读者，刚才构造的模 $V[x]$ 不过是 $k[x] \otimes_k V$. 确实，下一引理就用了张量积与直和可交换的事实，这是因为子集 B 是 V 的基当且仅当 $V = \sum_{b \in B} kb$ 是直和.

引理 9.55 如果 V 是交换环 k 上的自由 k-模，则 $V[x]$ 是自由 $k[x]$-模. 事实上，V 的基 E 也是作为自由 $k[x]$-模的 $V[x]$ 的基.

证明 每个元素 $u \in V[x]$ 有形如 $u = \sum_{i \geqslant 0} x^i v_i$ 的表达式. 因 $x^i e_1, \cdots, x^i e_n$ 是 $V_i = x^i V$ 的基，每个 $v_i = \sum_j \alpha_{ji} e_j$，其中 $\alpha_{ji} \in k$. 合并同类项得

$$u = f_1(x) e_1 + \cdots + f_n(x) e_n,$$

684

其中 $f_j(x) = \alpha_{j0} + \alpha_{j1} x + \cdots + \alpha_{jt} x^t$，$t$ 是某个整数.

为证明这个表达式的唯一性，假设

$$g_1(x) e_1 + \cdots + g_n(x) e_n = 0,$$

其中 $g_j(x) = \beta_{j0} + \beta_{j1} x + \cdots + \beta_{jt} x^t$，$t$ 是某个整数，这个等式对每个 i 给出 V_i 中的等式. $\sum_j \beta_{ji} x^i e_j = 0$. 因 $x^i e_1, \cdots, x^i e_n$ 是 V_i 的基，它们线性无关，所以一切 $\beta_{ji} = 0$. ■

现在可以给出 V^T 的有限表现. 在这个证明中把 $V[x]$ 看作序列较方便（比看作 $k[x] \otimes_k V$ 方便）.

定理 9.56（特征序列） （ⅰ）如果 V 是交换环 k 上的有限生成 k-模，且 $T: V \to V$ 是 k-同态，则存在 $k[x]$-模的正合列

$$0 \to V[x] \xrightarrow{\lambda} V[x] \xrightarrow{\pi} V^T \to 0,$$

其中对一切 $i\geqslant 0$ 和一切 $v\in V,\lambda(x^iv)=x^{i+1}v-x^iTv$ 和 $\pi(x^iv)=T^iv$.

(ⅱ) 如果 A 是 k 上的 $n\times n$ 矩阵和 E 是 k^n 的标准基 $E=e_1,\cdots,e_n$，则(ⅰ)中 $(k^n)^A$ 的表现形成的矩阵 ${}_E[\lambda]_E$ 是 $xI-A$.

证明 (ⅰ) 容易验证 λ 和 π 都是合理定义的 k-映射；它们也是 $k[x]$-映射；例如，

$$\lambda(x(x^iv))=x\lambda(x^iv),$$

这是因为两端都等于 $x^{i+2}v-x^{i+1}Tv$.

(1) π 是满射. 如果 $v\in V^T$，则 $\pi(v)=T^0v=v$.

(2) $\mathrm{im}\lambda\subseteq\ker\pi$.

$$\pi\lambda(x^iv)=\pi(x^{i+1}v-x^iTv)=T^{i+1}v-T^{i+1}v=0.$$

(3) $\ker\pi\subseteq\mathrm{im}\lambda$. 如果 $u=\sum_{i=0}^{m}x^iv_i\in\ker\pi$，则 $\sum_{i=0}^{m}T^iv_i=0$. 因此，

$$\begin{aligned}u&=\sum_{i=0}^{m}x^iv_i-\sum_{i=0}^{m}T^iv_i\\&=\sum_{i=1}^{m}(x^iv_i-T^iv_i),\end{aligned}$$

这是因为

$$x^0v_0-T^0v_0=v_0-v_0=0.$$

对任意 $i\geqslant 1$，我们改写 u 的第 i 个直和项 $x^iv_i-T^iv_i$ 为重叠和，它的每个项都在 $\mathrm{im}\lambda$ 中；这就足以证明 $\ker\pi\subseteq\mathrm{im}\lambda$. [685]

$$\begin{aligned}\sum_{j=0}^{i-1}\lambda(x^{i-1-j}T^jv_i)&=\sum_{j=0}^{i-1}(x^{i-j}T^jv_i-x^{i-1-j}T^{j+1}v_i)\\&=(x^iv_i-x^{i-1}Tv_i)+(x^{i-1}Tv_i-x^{i-2}T^2v_i)\\&\quad+\cdots+(xT^{i-1}v_i-T^iv_i)\\&=x^iv_i+\Big[\sum_{j=1}^{i-1}(-x^{i-j}T^jv_i+x^{i-j}T^jv_i)\Big]-T^iv_i\\&=x^iv_i-T^iv_i.\end{aligned}$$

(4) λ 是单射. 作为 k-模，$V[x]$ 是子模 V_i 的直和，且对一切 $m\geqslant 0$，经 $f_m:x^mv\mapsto v$ 有 $V_m\cong V$；由此，如果 $x^mv\neq 0$，则 $f_{m+1}^{-1}f_m(x^mv)=x^{m+1}v\neq 0$.

现在假设

$$u=\sum_{i=0}^{m}x^iv_i\in\ker\lambda.$$

其中 $x^mv_m\neq 0$；由此 $x^{m+1}v_m\neq 0$. 但

$$0=\lambda(u)=\lambda\Big(\sum_{i=0}^{m}x^iv_i\Big)=\sum_{i=0}^{m}(x^{i+1}v_i-x^iTv_i).$$

所以，

$$x^{m+1}v_m=-\sum_{i=0}^{m-1}(x^{i+1}v_i)+\sum_{i=0}^{m}x^iTv_i.$$

于是，$x^{m+1}v_m\in V_{m+1}\cap\sum_{i=0}^{m}V_i=\{0\}$，从而 $x^{m+1}v_m=0$. 但我们已经看到 $x^mv_m\neq 0$ 蕴涵

$x^{m+1}v_m \neq 0$，因此这个矛盾给出 $\ker\lambda = \{0\}$.

（ii）在（i）的记号中，令 $V = k^n$ 和 $T: k^n \to k^n$ 为 $v \mapsto Av$，其中 v 是 $n\times 1$ 列向量. 如果 $e_1, \cdots, e_n$ 是 k^n 的标准基，则 $e_1, \cdots, e_n$ 是自由 $k[x]$-模 $V[x]$ 的基，因此只需找出 λ 关于这组基的矩阵. 现在

$$\lambda(e_i) = xe_i - Te_i = xe_i - \sum_j a_{ji}e_j.$$

因 $[\delta_{ij}] = I$，其中 δ_{ij} 是克罗内克 δ，有

$$\begin{aligned} xe_i - \sum_j a_{ji}e_j &= \sum_j x\delta_{ji}e_j - \sum_j a_{ji}e_j \\ &= \sum_j (x\delta_{ji} - a_{ji})e_j. \end{aligned}$$

686 所以 λ 的矩阵是 $xI - A$. ■

系 9.57 域 k 上的两个 $n\times n$ 矩阵 A 和 B 相似当且仅当矩阵 $\Gamma = xI - A$ 和 $\Gamma' = xI - B$ 是 $k[x]$-等价的.

证明 如果 A 和 B 相似，则存在元素在 k 中的非奇异矩阵 P 使得 $B = PAP^{-1}$. 但因标量矩阵 xI 和 P 可交换（xI 和每个矩阵都可交换），有

$$P(xI - A)P^{-1} = xI - PAP^{-1} = xI - B.$$

于是，$xI - A$ 和 $xI - B$ 是 $k[x]$-等价的.

反之，假设矩阵 $xI - A$ 和 $xI - B$ 是 $k[x]$-等价的. 根据定理 9.56（ii），$(k^n)^A$ 和 $(k^n)^B$ 是有限表现 $k[x]$-模，它们的表现分别给出矩阵 $xI - A$ 和 $xI - B$. 现在命题 9.54 证明 $(k^n)^A \cong (k^n)^B$，因此根据系 7.4，A 和 B 相似. ■

系 9.57 把域 k 上的矩阵的相似性问题简化为 $k[x]$ 上矩阵的等价问题. 有幸的是**高斯消元法**（解系数在域中的线性方程组的一种方法）可以修改而适用于此. 现在把高斯消元法的要素从域上的矩阵推广到任意交换环上的矩阵.

下面，我们记矩阵 A 的第 i 行为 ROW(i)，第 j 列为 COL(j).

定义 元素在交换环 R 中的矩阵 A 的三种**初等行运算**是指：

Ⅰ型：ROW(j) 乘以单位 $u \in R$.

Ⅱ型：把 ROW(i) 换成 ROW(i) + c_jROW(j)，其中 $j \neq i$ 和 $c_j \in R$.

Ⅲ型：交换 ROW(i) 和 ROW(j).

类似有**初等列运算**.

注意，一个Ⅲ型运算（即一个交换）可以用另外两个类型的运算完成. 示意如下：

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \to \begin{bmatrix} a-c & b-d \\ c & d \end{bmatrix} \to \begin{bmatrix} a-c & b-d \\ a & b \end{bmatrix} \to \begin{bmatrix} -c & -d \\ a & b \end{bmatrix} \to \begin{bmatrix} c & d \\ a & b \end{bmatrix}$$

定义 **初等矩阵**是指对单位矩阵作一个初等行运算[⊖]得到的矩阵.

于是，有三种类型的初等矩阵. 在初等线性代数课程中证明（证明是容易的）实施一个初等运算和乘以一个初等矩阵是一样的. 详细地说，如果 L 是一个Ⅰ，Ⅱ或Ⅲ型初等矩阵，则对矩阵 A 实施某型的初等行运算给出矩阵 LA，而对 A 实施对应的初等列运算给出矩阵 AL. 也容易看出每个初等矩阵都是可逆的，且它的逆是同类型的初等矩阵. 由此，初等矩阵的积是可逆的.

687

⊖ 对 I 应用初等列运算得到相同的初等矩阵集合.

定义 如果 R 是交换环，则矩阵 Γ' 和矩阵 Γ 称为**高斯等价**，如果存在初等行运算和初等列运算的序列使得

$$\Gamma=\Gamma_0\to\Gamma_1\to\cdots\to\Gamma_r=\Gamma'.$$

高斯等价是 R 上的一切 $n\times t$ 矩阵族上的等价关系．

由此，如果 Γ' 高斯等价于 Γ，则存在矩阵 P 和 Q 使得 $\Gamma'=P\Gamma Q$，其中 P，Q 都是初等矩阵的积．回忆两个矩阵 Γ' 和 Γ 是 R-等价的，如果存在可逆矩阵 P 和 Q 使得 $\Gamma'=P\Gamma Q$．由此，如果 Γ' 高斯等价于 Γ，则 Γ' 和 Γ R-等价．我们将看到当 R 是欧几里得环时，逆命题也真．

定理 9.58（史密斯[⊖]正规型） 元素在欧几里得环 R 中的每个非零 $n\times t$ 矩阵 Γ 高斯等价于形如

$$\begin{bmatrix}\Sigma & 0\\ 0 & 0\end{bmatrix}$$

的矩阵，其中 $\Sigma=\operatorname{diag}(\sigma_1,\cdots,\sigma_q)$ 且 $\sigma_1\mid\sigma_2\mid\cdots\mid\sigma_q$ 是非零的（下面为 0 的块或右面为 0 的块可以不出现）．

证明 对 Γ 的行数 $n\geqslant 1$ 用归纳法证明．如果 $\sigma\in R$，令 $\partial(\sigma)$ 表示它在欧几里得环 R 中的次数．在与 Γ 高斯等价的矩阵的一切元素中，设 σ_1 有最小次数，并设 Δ 是与 Γ 高斯等价且有元素 σ_1 的矩阵，比如 σ_1 位于 k,ℓ．

我们断言在 Δ 的 $\mathrm{ROW}(k)$ 中，对一切 η_{kj} 有 $\sigma_1\mid\eta_{kj}$．否则存在 $j\neq\ell$ 和等式 $\eta_{kj}=\kappa\sigma_1+\rho$，其中 $\partial(\rho)<\partial(\sigma_1)$．把 $(-\kappa)\mathrm{COL}(\ell)$ 加到 $\mathrm{COL}(j)$ 得有元素 ρ 的矩阵 Δ'．但 Δ' 高斯等价于 Γ 且有次数小于 $\partial(\sigma_1)$ 的元素 ρ，这就产生矛盾．同样的论证可以证明 σ_1 整除它所在列的任一元素．我们断言 σ_1 整除 Δ 的每个元素．设 a 是不在 σ_1 的行也不在 σ_1 的列的元素；示意论证如下，比如有 $\begin{bmatrix}a & b\\ c & \sigma_1\end{bmatrix}$，其中 $b=u\sigma_1$ 和 $c=v\sigma_1$．把 $\mathrm{ROW}(1)$ 换成 $\mathrm{ROW}(1)+(1-u)\mathrm{ROW}(2)=(a+(1-u)c\,\sigma_1)$．如上所示，$\sigma_1\mid a+(1-u)c$．因 $\sigma_1\mid c$，有 $\sigma_1\mid a$．

我们回到 Δ，这是一个和 Γ 高斯等价且包含元素 σ_1 的矩阵．作交换得到和 Γ 高斯等价且 1,1 位置的元素为 σ_1 的矩阵 Δ'．如果 η_{1j} 是第一行中的另一个元素，则 $\eta_{1j}=\kappa_j\sigma_1$，把 $(-\kappa_j)\ \mathrm{COL}(1)$ 加到 $\mathrm{COL}(j)$ 得到 1，j 元素为 0 的新矩阵．于是，矩阵 Δ 高斯等价于这样的一个矩阵，它的 1,1 位置是 σ_1，第一行的其他元素是 0．由此，我们已经证明了一个非零 $1\times t$ 矩阵和 $[\sigma_1,0,\cdots,0]$ 高斯等价，从而完成了归纳法中基础步 $n=1$ 的证明．进一步，因 σ_1 整除第一列中的一切元素，所以 Γ 高斯等价于第一列的其余元素全是 0 的一个矩阵；于是，Γ 高斯等价于形如 [688]

$$\begin{bmatrix}\sigma_1 & 0\\ 0 & \Omega\end{bmatrix}$$

的矩阵．根据归纳假设，矩阵 Ω 高斯等价于矩阵

$$\begin{bmatrix}\Sigma' & 0\\ 0 & 0\end{bmatrix},$$

其中 $\Sigma'=\operatorname{diag}(\sigma_2,\cdots,\sigma_q)$ 且 $\sigma_2\mid\sigma_3\mid\cdots\mid\sigma_q$．因此，$\Gamma$ 和 $\begin{bmatrix}\sigma_1 & 0 & 0\\ 0 & \Sigma' & 0\\ 0 & 0 & 0\end{bmatrix}$ 高斯等价．剩下要考察 $\sigma_1\mid\sigma_2$；

⊖ 立即要证明的这个定理以及对应的唯一性结果于 1861 年由史密斯发现．

这来自我们开始的说明，因为最终的矩阵和 Γ 高斯等价且包含元素 σ_1. ■

定义 定理陈述中的矩阵 $\begin{bmatrix}\Sigma & 0\\0 & 0\end{bmatrix}$ 称为 Γ 的**史密斯正规型**.

于是，定理说元素在欧几里得环 R 中的每个非零（长方）矩阵和一个史密斯正规型高斯等价.

系 9.59 设 R 是欧几里得环.

（ⅰ）元素在 R 中的每个可逆 $n\times n$ 矩阵 Γ 都是初等矩阵的积.

（ⅱ）R 上的两个矩阵 Γ 和 Γ' R-等价当且仅当它们高斯等价.

证明 （ⅰ）我们现在知道 Γ 和一个史密斯正规型 $\begin{bmatrix}\Sigma & 0\\0 & 0\end{bmatrix}$ 高斯等价，其中 Σ 是对角矩阵. 因 Γ 是(方)可逆矩阵，不可能有 0 的块，因此 Γ 和 Σ 高斯等价；即存在矩阵 P 和 Q，P 和 Q 都是初等矩阵的积，使得

$$P\Gamma Q=\Sigma=\operatorname{diag}(\sigma_1,\cdots,\sigma_n).$$

因此，$\Gamma=P^{-1}\Sigma Q^{-1}$. 现在，初等矩阵的逆也是初等矩阵，因此 P^{-1} 和 Q^{-1} 是初等矩阵的积. 因 Σ 可逆，$\det(\Sigma)=\sigma_1\cdots\sigma_n$ 是 R 中的单位. 由此，每个 σ_i 都是单位，从而 Σ 是 n 个初等矩阵的积 [由 ROW(i) 乘以单位 σ_i 的初等变换得到].

689

（ⅱ）如果 Γ' 和 Γ 高斯等价，则它们 R-等价，这个论断总是成立的，因为如果 $\Gamma'=P\Gamma Q$，其中 P 和 Q 是初等矩阵的积，则 P 和 Q 可逆. 反之，如果 Γ' 和 Γ R-等价，则 $\Gamma'=P\Gamma Q$，其中 P 和 Q 可逆，（ⅰ）证明 Γ' 和 Γ 高斯等价. ■

有例子证明这个命题对不是欧几里得环[⊖]的 PID 不成立. 研究这一现象在代数 K-理论的开端很重要（见 Milnor 所著的《Introduction to Algebraic K-Theory》.

定理 9.60（同步基） 设 R 是欧几里得环，设 F 是有限生成自由 R-模，并设 S 是 F 的子模，则存在 F 的基 $z_1,\cdots,z_n$ 和 R 中的非零元素 $\sigma_1,\cdots,\sigma_q$，其中 $0\leqslant q\leqslant n$，满足 $\sigma_1\mid\cdots\mid\sigma_q$，且 $\sigma_1z_1,\cdots,\sigma_qz_q$ 是 S 的基.

证明 如果 $M=F/S$，则系 9.4 证明 S 是自由的且秩 $\leqslant n$，由此，

$$0\to S\xrightarrow{\lambda}F\to M\to 0$$

是 M 的表现，其中 λ 是包含映射. 现在对 S 和 F 任意选取的基相伴于 λ 所对应的一个矩阵 Γ（注意 Γ 可以是长方的）. 根据命题 9.53，存在 S 和 F 的新基，在这新基下，Γ R-等价于一个史密斯正规型，而这个新基正是定理中所描述的. ■

系 9.61 设 Γ 是元素在欧几里得环 R 中的 $n\times n$ 矩阵.

（ⅰ）如果 Γ 和形如 $\operatorname{diag}(\sigma_1,\cdots,\sigma_q)\oplus 0$ 的史密斯正规型 R-等价，则不是单位的那些 $\sigma_1,\cdots,\sigma_q$ 是 Γ 的不变因子.

（ⅱ）如果 $\operatorname{diag}(\eta_1,\cdots,\eta_s)\oplus 0$ 是 Γ 的另一个史密斯正规型，则 $s=q$ 且对一切 i，存在单位 u_i 使得 $\eta_i=u_i\sigma_i$；即对角线元素是相伴的.

证明 （ⅰ）我们可以把 Γ 看作 R-映射 $\lambda: R^n\to R^n$ 关于某组基的矩阵. 设 $M=R^n/\operatorname{im}\lambda$. 如果 $\operatorname{diag}(\sigma_1,\cdots,\sigma_q)\oplus 0$ 是 Γ 的史密斯正规型，则存在 R^n 的基 $y_1,\cdots,y_n$ 和 R^n 的基 $z_1,\cdots,z_n$ 使得 $\lambda(y_1)=\sigma_1z_1,\cdots,\lambda(y_q)=\sigma_qz_q$，并且对一切 $j>q$，如果有的话，$\lambda(y_j)=0$. 如果 σ_s 为不是单位的第

⊖ 对一般 PID 有一种说法，它是用次等矩阵讨论初等矩阵的集合得到的；见习题 9.50.

一个 σ_i，则

$$M \cong R^{n-q} \oplus R/(\sigma_s) \oplus \cdots \oplus R/(\sigma_q),$$

它是一个循环模的直和且 $\sigma_s \mid \cdots \mid \sigma_q$. 有限生成 R-模的基本定理使得 σ_s，…，σ_q 等同于 M 的不变因子.

（ii）由（i）证明了史密斯正规型实质上的唯一性，这是因为作为阶理想生成元的不变因子如不计相伴是唯一确定的. ■ 690

稍微泛用语言，我们可以论及一个矩阵的史密斯正规型.

系 9.62 域 k 上的两个 $n\times n$ 矩阵 A 和 B 相似当且仅当 $xI-A$ 和 $xI-B$ 在 $k[x]$上有相同的史密斯正规型.

证明 根据定理 9.57，A 和 B 相似当且仅当 $xI-A$ 和 $xI-B$ 是 $k[x]$-等价的，系 9.61 证明 $xI-A$ 和 $xI-B$ 是 $k[x]$-等价的当且仅当它们有相同的史密斯正规型. ■

系 9.63 设 F 是有限生成自由阿贝尔群，并设 S 是 F 的有有限指数的子群；设 y_1，…，y_n 是 F 的基，设 z_1，…，z_n 是 S 的基，并设 $A=[a_{ij}]$是满足 $z_i=\sum_j a_{ji}y_j$ 的 $n\times n$ 矩阵. 则

$$[F : S] = |\det(A)|.$$

证明 改变 S 和 F 的基把 A 变成和它$\mathbb{Z}$-等价的矩阵 B：

$$B = QAP,$$

其中 Q 和 P 是元素在$\mathbb{Z}$中的可逆矩阵. 因$\mathbb{Z}$中的单位只有 1 和 -1，所以有 $|\det(B)|=|\det(A)|$. 特别地，如果选取 B 为史密斯正规型，则 $B=\operatorname{diag}(g_1,\cdots,g_n)$，从而 $|\det(B)|=g_1\cdots g_n$. 但 $g_1,\cdots,g_n$ 是 F/S 的不变因子；根据系 5.30，它们的积是 F/S 的阶，也就是指数$[F : S]$. ■

我们还未曾兑现承诺以给出算法计算元素在域上的矩阵的不变因子.

定理 9.64 设 $\Sigma=\operatorname{diag}(\sigma_1,\cdots,\sigma_q)$是矩阵 Γ 的史密斯正规型中的对角块，其中 Γ 的元素在欧几里得环 R 上. 如果定义 $d_i(\Gamma)$ 为 $d_0(\Gamma)=1$，且对 $i>0$，

$$d_i(\Gamma) = \gcd(\Gamma \text{ 的一切 } i\times i \text{ 子式}),$$

则对一切 $i\geqslant 1$，

$$\sigma_i = d_i(\Gamma)/d_{i-1}(\Gamma).$$

证明 我们证明如果 Γ 和 Γ' R-等价，则对一切 i，

$$d_i(\Gamma) \sim d_i(\Gamma'),$$

其中记号 $a\sim b$ 表示 a 和 b 在 R 中是相伴的. 这样就足以证明定理了，因为如果 Γ'是 Γ 的史密斯正规型，它的对角块是 $\operatorname{diag}(\sigma_1,\cdots,\sigma_q)$，则 $d_i(\Gamma')=\sigma_1\sigma_2\cdots\sigma_i$. 因此

$$\sigma_i(x) = d_i(\Gamma')/d_{i-1}(\Gamma') \sim d_i(\Gamma)/d_{i-1}(\Gamma).$$ 691

根据命题 9.59，只要证明对每个初等矩阵 L 有

$$d_i(\Gamma) \sim d_i(L\Gamma) \text{ 和 } d_i(\Gamma) \sim d_i(\Gamma L).$$

确实，只要证明 $d_i(\Gamma L)\sim d_i(\Gamma)$，这是因为 $d_i(\Gamma L)=d_i([\Gamma L]^t)=d_i(L^t\Gamma^t)$ [Γ^t的 $i\times i$ 子矩阵是 Γ 的 $i\times i$ 子矩阵的转置；现在用事实：L^t 是初等矩阵，且对每个方矩阵 M，$\det(M^t)=\det(M)$].

最后还可简化，只需考虑 I 型和 II 型初等运算，因为我们已经看到 III 型初等运算（交换两行）可以用其他两个类型来完成.

L 是 I 型初等矩阵.

如果 Γ 的 $\mathrm{ROW}(\ell)$乘以单位 u，则一个 $i\times i$ 子矩阵或者保持不变，或者它的一行乘以 u. 在第一

种情形中，子式（就是它的行列式）保持不变；在第二种情形中，子式改变一个单位 u. 所以，$L\Gamma$ 的每个 $i\times i$ 子式是 Γ 的对应 $i\times i$ 子式的相伴，从而 $d_i(L\Gamma)\sim d_i(\Gamma)$.

L 是Ⅱ型初等矩阵 .

如果 L 把 $\mathrm{ROW}(\ell)$ 换成 $\mathrm{ROW}(\ell)+r\mathrm{ROW}(j)$ ，则只有 Γ 的 $\mathrm{ROW}(\ell)$ 有改变. 于是，Γ 的一个 $i\times i$子式或者不涉及这行，或者涉及这行. 在第一种情形中，$L\Gamma$ 的对应子式不变；在第二种情形中，子式形如 $m+rm'$，其中 m 和 m'都是 Γ 的 $i\times i$ 子式（因为行列式是矩阵行的多重线性函数). 因为 $d_i(\Gamma)\mid m$ 和 $d_i(\Gamma)\mid m'$ ，所以 $d_i(\Gamma)\mid d_i(L\Gamma)$. 因 L^{-1} 也是Ⅱ型初等矩阵，这个论证表明 $d_i(L^{-1}(L\Gamma))\mid d_i(L\Gamma)$. 当然，$L^{-1}(L\Gamma)=\Gamma$ ，从而 $d_i(\Gamma)$ 和 $d_i(L\Gamma)$ 相互整除. 因 R 是整环，有 $d_i(L\Gamma)\sim d_i(\Gamma)$. ■

定理 9.65 *存在计算元素在域 k 中的任意方矩阵 A 的初等因子的算法 .*

证明 根据系 9.62，只要求出环 $k[x]$ 上的 $\Gamma=xI-A$ 的史密斯正规型；根据系 9.61，A 的不变因子就是不是单位的对角线元素.

有两种算法：对一切 i，计算 $d_i(xI-A)$（当然，对大矩阵这不是一个十分有效的算法）；用 $k[x]$ 上的高斯消元法把 $xI-A$ 变成史密斯正规型 . 读者现在不难写出计算初等因子的程序. ■

例 9.66 求

$$A=\begin{bmatrix}2&3&1\\1&2&1\\0&0&-4\end{bmatrix}$$

692

在$\mathbb{Q}$上的不变因子 . 我们把两种计算模式组合起来运用：高斯消元法和子式的 gcd 法. 现在

$$xI-A=\begin{bmatrix}x-2&-3&-1\\-1&x-2&-1\\0&0&x+4\end{bmatrix}.$$

显然 $g_1=1$，这是因为 A 的元素中有一些非零常数，从而它是 A 的一切元素的 gcd. 交换 ROW(1) 和 ROW(2)，并把第一行变号得

$$\begin{bmatrix}1&-x+2&1\\x-2&-3&-1\\0&0&x+4\end{bmatrix}.$$

把 $-(x-2)\mathrm{ROW}(1)$ 加到 ROW(2) 得

$$\begin{bmatrix}1&-x+2&1\\0&x^2-4x+1&-x+1\\0&0&x+4\end{bmatrix}\to\begin{bmatrix}1&0&0\\0&x^2-4x+1&-x+1\\0&0&x+4\end{bmatrix}.$$

2×2 子矩阵

$$\begin{bmatrix}x^2-4x+1&-x+1\\0&x+4\end{bmatrix}$$

中元素的 gcd 是 1，这是因为 $-x+1$ 和 $x+4$ 是不同的不可约多项式，因此 $g_2=1$. 我们已经证明了 A 的不变因子只有一个，就是 $(x^2-4x+1)(x+4)=x^3-15x+4$ ，而且它必是 A 的特征多项式. 由此，A 的特征多项式和极小多项式一致，系 9.43 证明 A 的有理典范型是

$$\begin{bmatrix}0 & 0 & -4\\ 1 & 0 & 15\\ 0 & 1 & 0\end{bmatrix}.$$

■

例 9.67 求有生成元 a，b，c 和关系

$$7a+5b+2c=0$$
$$3a+3b=0$$
$$13a+11b+2c=0$$

的阿贝尔群 G. 用Z上的初等运算求关系矩阵的史密斯正规型：

$$\begin{bmatrix}7 & 5 & 2\\ 3 & 3 & 0\\ 13 & 11 & 2\end{bmatrix}\to\begin{bmatrix}1 & 0 & 0\\ 0 & 6 & 0\\ 0 & 0 & 0\end{bmatrix}.$$

由此，$G\cong(\mathbf{Z}/1\,\mathbf{Z})\oplus(\mathbf{Z}/6\,\mathbf{Z})\oplus(\mathbf{Z}/0\,\mathbf{Z})$. 化简得 $G\cong \mathbf{I}_6\oplus\mathbf{Z}$. ■ 693

习题

9.47 求矩阵

$$\begin{bmatrix}-4 & 6 & 3\\ -3 & 5 & 4\\ 4 & -5 & 3\end{bmatrix}$$

在Q上的不变因子.

9.48 求矩阵

$$\begin{bmatrix}-6 & 2 & -5 & -19\\ 2 & 0 & 1 & 5\\ -2 & 1 & 0 & -5\\ 3 & -1 & 2 & 9\end{bmatrix}$$

在Q上的不变因子.

9.49 如果 k 是域，证明存在加性正合函子 ${}_k\mathbf{Mod}\to{}_{k[x]}\mathbf{Mod}$ 把任一向量空间 V 变到 $V[x]$. [见定理 9.56 (ⅱ).]

9.50 设 R 是 PID，并设 a，$b\in R$.

(ⅰ) 如果 d 是 a 和 b 的 gcd，证明存在 $\det(Q)=1$的 2×2 矩阵 $Q=\begin{bmatrix}x & y\\ x' & y'\end{bmatrix}$使得

$$Q\begin{bmatrix}a & *\\ b & *\end{bmatrix}=\begin{bmatrix}d & *\\ d' & *\end{bmatrix},$$

其中 $d\mid d'$.

提示：如果 $d=xa+yb$，定义 $x'=b/d$ 和 $y'=-a/d$.

(ⅱ) $n\times n$ 矩阵 U 称为**次等矩阵**，如果它可以划分为

$$U=\begin{bmatrix}Q & 0\\ 0 & I\end{bmatrix},$$

其中 Q 是行列式为 1 的 2×2 矩阵. 证明元素在 PID 中的每个 $n\times n$ 矩阵 A 可以被一系列初等和次等矩阵变为史密斯正规型.

9.5 双线性型

本节中 k 是域，V 是 k 上的向量空间，通常是有限维的. 即使还没有证明行列式的基本定理（它们将在 9.9 节证明），我们还是继续使用它们熟知的性质.

定义 V 上的一个**双线性型**（或**内积**）是指一个双线性函数

$$f: V\times V \to k.$$

694 有序对(V,f)叫做**内积空间**.

当然，如果 f 是熟知的点积

$$f(u,v)=\sum_i u_i v_i,$$

则(k^n,f)是内积空间，其中 $u=(u_1,\cdots,u_n)^t$ 和 $v=(v_1,\cdots,v_n)^t$（上标 t 表示转置；记住 k^n 中的元素是$n\times 1$ 列向量）. 用矩阵乘法表示有

$$f(u,v)=u^t v.$$

有两种类型的双线性型特别重要.

定义 如果一个双线性型 $f: V\times V\to k$ 对一切 u，$v\in V$ 有

$$f(u,v)=f(v,u),$$

则称 f 是**对称的**. 当 f 对称时，我们称内积空间(V,f)为**对称空间**.

如果对一切 $v\in V$ 有 $f(v,v)=0$，则称双线性型 f 是**交错的**. 当 f 交错时，我们称内积空间(V,f)为**交错空间**.

例 9.68 （i）如果 $V=k^2$ 并把它的元素看作列向量，则由

$$\left(\begin{bmatrix}a\\b\end{bmatrix},\begin{bmatrix}c\\d\end{bmatrix}\right)\mapsto \det\begin{bmatrix}a & c\\ b & d\end{bmatrix}=ad-bc$$

给出的 $\det: V\times V\to k$ 是交错双线性型的一例.

（ii）在第 8 章中，我们在有限群 G 上一切类函数的复向量空间 $\mathrm{cf}(G)$ 上定义了一个（埃尔米特）型. 更一般地，定义函数 $f:\mathbb{C}^n\times\mathbb{C}^n\to\mathbb{C}$ 为

$$f(u,v)=\sum_j u_j\bar{v}_j,$$

其中 $u=(u_1,\cdots,u_n)^t, v=(v_1,\cdots,v_n)^t$，$\bar{c}$ 表示复数 c 的复共轭. 因为 $f(u,cv)=\bar{c}f(u,v)$ 而不是 $cf(u,v)$，所以这个函数不是$\mathbb{C}$-双线性的. 埃尔米特型是半线性型的例子；这样的型可以在任意域 k 上配置一个 2 阶自同态（扮演复共轭的角色）构造出来. ■

695 每个双线性型可以用对称双线性型和交错双线性型表示.

命题 9.69 设 k 是特征$\neq 2$ 的域，并设 f 是定义在 k 上的向量空间 V 上的双线性型，则存在唯一的双线性型 f_s 和 f_a 使得 $f=f_s+f_a$，其中 f_s 是对称的，f_a 是交错的.

证明 根据假设，$\frac{1}{2}\in k$，因此可以定义

$$f_s(u,v)=\frac{1}{2}(f(u,v)+f(v,u))$$

和

$$f_a(u,v)=\frac{1}{2}(f(u,v)-f(v,u)).$$

显然 $f=f_s+f_a$，且 f_s是对称的，f_a是交错的. 现在证明唯一性. 如果 $f=f_s'+f_a'$，其中 f_s'是对称的，f_a'是交错的，则 $f_s+f_a=f_s'+f_a'$，从而 $f_s-f_s'=f_a'-f_a$. 如果定义 g 为共同的值，即 $f_s-f_s'=g=f_a'-f_a$，则 g 既是对称的又是交错的. 根据习题 9.54，$g=0$，从而 $f_s=f_s'$和 $f_a=f_a'$. ■

注 如果(V,g)是内积空间，则 g 称为**反称的**，如果对一切 u，$v\in V$ 有

$$g(v,u)=-g(u,v).$$

我们现在证明，如果 k 的特征不是 2，则 g 是交错的当且仅当 g 是反称的.

如果 g 是任意双线性型，则有

$$g(u+v,u+v)=g(u,u)+g(u,v)+g(v,u)+g(v,v).$$

所以，如果 g 是交错的，则 $0=g(u,v)+g(v,u)$，因此 g 是反称的.（我们还没有用到假设 k 的特征不为 2.）

反之，如果 g 是反称的，则在等式 $g(u,v)=-g(v,u)$ 中令 $u=v$ 得 $g(u,u)=-g(u,u)$；即 $2g(u,u)=0$. 因 k 的特征不是 2，所以 $g(u,u)=0$，从而 g 是交错的.

定义 设 f 是域k 上向量空间 V 上的双线性型，并设 $E=e_1,\cdots,e_n$ 是 V 的基，则 f **关于**E **的内积矩阵**是指

$$A=[f(e_i,e_j)].$$

假设(V,f)是内积空间，$e_1,\cdots,e_n$ 是 V 的基，$A=[f(e_i,e_j)]$是 f 关于 E 的内积矩阵. 如果$b=\sum b_ie_i$ 和 $c=\sum c_ie_i$ 是 V 中的向量，则

$$f(b,c)=f(\sum b_ie_i,\sum c_ie_i)=\sum_{i,j}b_if(e_i,e_j)c_j.$$

如果 B 和 C 分别表示列向量$(b_1,\cdots,b_n)^t$ 和$(c_1,\cdots,c_n)^t$，则上面的等式可以写成矩阵形式：

$$f(b,c)=B^tAC.$$

于是，内积矩阵完全确定了 f. 696

命题 9.70 设 V 是域k 上的 n 维向量空间.

（ⅰ）域k 上的每个 $n\times n$ 矩阵 A 都是定义在 $V\times V$ 上的某个双线性型 f 的内积矩阵. 如果 f 是对称的，则关于 V 的任意一个基，它的内积矩阵 A 是对称矩阵（即 $A^t=A$）. 如果 f 是交错的，则关于 V 的任意一个基的内积矩阵是反称的（即 $A^t=-A$）.

（ⅱ）如果对一切列向量 B 和 C，$B^tAC=B^tA'C$，则 $A=A'$.

（ⅲ）设 A 和A'分别是 V 上双线性型 f 和 f'关于基 E 和 E'的内积矩阵，则 $f=f'$当且仅当 A 和 A'是**相合的**；即存在非奇异矩阵 P 使得

$$A'=P^tAP.$$

证明 （ⅰ）对任一矩阵 A，易知由 $f(b,c)=b^tAc$ 定义的函数 $f: k^n\times k^n\to k$ 是一个双线性型，且 A 是它关于标准基 $e_1,\cdots,e_n$ 的内积矩阵. 读者容易把这个构造转移到选定了基的任意向量空间 V 上.

如果 f 是对称的，则它的内积矩阵 $A=[a_{ij}]$也是对称的，这是因为 $a_{ij}=f(e_i,e_j)=f(e_j,e_i)=a_{ji}$；类似地，如果 f 是交错的，则 $a_{ij}=f(e_i,e_j)=-f(e_j,e_i)=-a_{ji}$.

（ⅱ）如果 $b=\sum_i b_ie_i$ 和 $c=\sum_i c_ie_i$，则我们已经知道 $f(b,c)=B^tAC$，其中 B 和 C 是 b 和 c 关于 E 的坐标的列向量. 特别地，如果 $b=e_i$ 和 $c=e_j$，则 $f(e_i,e_j)=a_{ij}$ 是 A 的 ij 元素.

(iii) 设 b 和 c 关于基 E' 的坐标分别是 B' 和 C'，因此 $f'(b,c)=(B')^tA'C'$，其中 $A'=[f(e_i',e_j')]$. 如果 P 是变换矩阵 ${}_E[1]_{E'}$，则 $B=PB'$ 和 $C=PC'$. 因此，$f(b,c)=B^tAC=(PB')^tA(PC')=(B')^t(P^tAP)C'$. 根据 (ii)，必有 $P^tAP=A'$.

反之，由给出的矩阵等式 $A'=P^tAP$ 产生等式：

$$
\begin{aligned}
[f'(e_i',e_j')] &= A' \\
&= P^tAP \\
&= \Big[\sum_{\ell q} p_{\ell i} f(e_\ell,e_q) p_{qj}\Big] \\
&= \Big[f\Big(\sum_\ell p_{\ell i}e_\ell, \sum_q p_{qj}e_q\Big)\Big] \\
&= [f(e_i',e_j')].
\end{aligned}
$$

因此，对一切 i,j, $f'(e_i',e_j')=f(e_i',e_j')$，由此对一切 $b,c\in V$, $f'(b,c)=f(b,c)$. 所以，$f=f'$.

697 ■

系 9.71 如果(V,f)是内积空间，A 和 A' 是 f 关于 V 的不同基的内积矩阵，则存在非零$a\in k$使得

$$\det(A')=a^2\det(A).$$

从而，A' 非奇异当且仅当 A 非奇异.

证明 由下列事实得到：$\det(P^t)=\det(P)$；$\det(AB)=\det(A)\det(B)$；以及 P 非奇异当且仅当 $\det(P)\neq 0$. ■

最重要的双线性型是非退化的双线性型.

定义 如果双线性型 f 有非奇异的内积矩阵，则称 f 是**非退化的**.

例如，k^n 上的点积是非退化的，因为它关于标准基的内积矩阵是单位矩阵 I.

双线性型的判别式实质上就是它的内积矩阵的行列式. 然而，内积矩阵依赖于基的选取，因此我们的定义还必须复杂一点.

定义 如果 k 是域，则记它的非零元素的乘法群为 $k^\times$. 定义 $(k^\times)^2=\{a^2: a\in k^\times\}$. 双线性型 f 的**判别式**或者是 0，或者是

$$\det(A)(k^\times)^2\in k^\times/(k^\times)^2,$$

其中 A 是 f 的内积矩阵.

由系 9.71，f 的判别式是合理定义的. 但是我们经常不经意地说 $\det(A)$ 是 f 的判别式，其中 A 是 f 的某个内积矩阵.

下一定义用来刻画非退化性.

定义 如果 (V,f) 是内积空间和 $W\subseteq V$ 是 V 的子空间，则 W 的**左正交补**是指

$$W^{\perp L}=\{b\in V: f(b,w)=0, \text{对一切 } w\in W\};$$

W 的**右正交补**是指

$$W^{\perp R}=\{c\in V: f(w,c)=0, \text{对一切 } w\in W\}.$$

易知 $W^{\perp L}$ 和 $W^{\perp R}$ 都是 V 的子空间. 此外，如果 f 是对称的或交错的，则 $W^{\perp L}=W^{\perp R}$，此时我们写作 $W^\perp$.

设(V,f)是内积空间，并设 A 是 f 关于 V 的基 $e_1,\cdots,e_n$ 的内积矩阵. 我们断言 $b\in V^{\perp L}$ 当且仅当 b 是齐次方程组 $A^tx=0$ 的解. 如果 $b\in V^{\perp L}$，则对一切 j, $f(b,e_j)=0$. 记 $b=\sum_i b_ie_i$，我们知

道 $0=f(b,e_j)=f\left(\sum_i b_ie_i,e_j\right)=\sum_i b_if(e_i,e_j)$．写作矩阵形式，$b=(b_1,\cdots,b_n)^t$ 和 $b^tA=0$；转置得 b 是齐次方程组 $A^tx=0$ 的解．逆命题的证明留给读者．类似的论证证明 $c\in V^{\perp R}$ 当且仅当 c 是齐次方程组 $Ax=0$ 的解．

698

命题 9.72 如果 (V,f) 是内积空间，则 f 是非退化的当且仅当 $V^{\perp L}=\{0\}=V^{\perp R}$；即如果对一切 $c\in V$ 有 $f(b,c)=0$，则 $b=0$，以及如果对一切 $b\in V$ 有 $f(b,c)=0$，则 $c=0$．

证明 上面的注记表明 $b\in V^{\perp L}$ 当且仅当 b 是齐次方程组 $A^tx=0$ 的解．所以，$V^{\perp L}\neq\{0\}$ 当且仅当存在非平凡解 b，习题 3.70 证明存在非平凡解当且仅当 $\det(A^t)=0$．因 $\det(A^t)=\det(A)$，所以 f 退化．类似的论证证明 $V^{\perp R}\neq\{0\}$ 当且仅当 $Ax=0$ 存在非平凡解． ■

例 9.73 设 (V,f) 是内积空间，并设 $W\subseteq V$ 是子空间．有可能 f 是非退化的，而它的限制 $f\mid(W\times W)$ 是退化的．例如，设 $V=k^2$，并设 f 关于标准基 e_1,e_2 有内积矩阵 $A=\begin{bmatrix}0&1\\1&0\end{bmatrix}$．显然 A 非奇异，因此 f 非退化．另一方面，如果 $W=\langle e_1\rangle$，则 $f\mid(W\times W)=0$，因此它是退化的． ■

下面是用对偶空间描述非退化性的特性．这是十分自然的，因为如果 f 是域 k 上的向量空间 V 上的双线性型，则对任一固定的 $u\in V$，函数 $f(\ ,u):V\to k$ 是线性泛函．

命题 9.74 设 (V,f) 是内积空间，并设 $e_1,\cdots,e_n$ 是 V 的基，则 f 非退化当且仅当 $f(\ ,e_1),\cdots,f(\ ,e_n)$ 是对偶空间 V^* 的基（我们称后者为**对偶基**）．

证明 假定 f 非退化．因 $\dim(V^*)=n$，只要证明线性无关．如果存在标量 $c_1,\cdots,c_n$ 使得 $\sum_i c_if(\ ,e_i)=0$，则

$$\sum_i c_if(v,e_i)=0 \text{ 对一切 } v\in V.$$

如果定义 $u=\sum_i c_ie_i$，则对一切 v，$f(v,u)=0$，因此非退化给出 $u=0$．但 $e_1,\cdots,e_n$ 是线性无关表，从而一切 $c_i=0$；因此，$f(\ ,e_1),\cdots,f(\ ,e_n)$ 也线性无关，所以它是 V^* 的基．

反之，假定给定的线性泛函是 V^* 的基．如果对一切 $v\in V$ 有 $f(v,u)=0$，其中 $u=\sum_i c_ie_i$，则 $\sum_i c_if(\ ,e_i)=0$．因这些线性泛函是线性无关的，所以一切 $c_i=0$，从而 $u=0$；即 f 是非退化的． ■

系 9.75 如果 (V,f) 是内积空间，且 f 非退化，则每个线性泛函 $g\in V^*$ 存在唯一的 $u\in V$ 使得

$$g=f(\ ,u).$$

699

证明 设 $e_1,\cdots,e_n$ 是 V 的基，并设 $f(\ ,e_1),\cdots,f(\ ,e_n)$ 是它的对偶基．因 $g\in V^*$，存在标量 c_i 使得 $g=\sum_i c_if(\ ,e_i)$．如果定义 $u=\sum_i c_ie_i$，则 $g(v)=f(v,u)$．

为证明唯一性，假设 $f(\ ,u)=f(\ ,u')$．则对一切 $v\in V$，$f(v,u-u')=0$，从而 f 的非退化性给出 $u-u'=0$． ■

系 9.76 设 (V,f) 是内积空间，且 f 非退化．如果 $e_1,\cdots,e_n$ 是 V 的基，则存在 V 的基 $b_1,\cdots,b_n$ 使得

$$f(e_i,b_j)=\delta_{ij}.$$

证明 因 f 非退化，由 $v\mapsto f(\ ,v)$ 给出的函数 $V\to V^*$ 是同构．由此下图交换：

$$\begin{array}{ccc} V\times V & \xrightarrow{f} & k, \\ \varphi\downarrow & \nearrow \text{ev} & \\ V\times V^* & & \end{array}$$

其中 ev 是赋值函数 $(x,g)\mapsto g(x)$ 和 $\varphi:(x,y)\mapsto(x,f(\ \ ,y))$. 对每个 i，设 $g_i\in V^*$ 是第i个坐标的函数：如果 $v\in V$ 和 $v=\sum_j c_je_j$，则 $g_i(v)=c_i$. 根据系 9.75，存在 $b_1,\cdots,b_n\in V$ 使得对一切 $i,g_i=f(\ \ ,b_i)$. 图的交换性给出

$$f(e_i,b_j)=\text{ev}(e_i,g_j)=\delta_{ij}.$$ ■

命题 9.77 设(V,f)是内积空间，并设 W 是 V 的子空间. 如果 $f\mid(W\times W)$ 非退化，则

$$V=W\oplus W^{\perp R}=W\oplus W^{\perp L}.$$

注 我们并没有假定 f 自身是非退化的；在例 9.73 中已经看到，即使假定 f 非退化，也不能保证 $f\mid(W\times W)$ 非退化.

证明 如果 $u\in W\cap W^\perp$，则对一切 $w\in W,f(w,u)=0$. 因 $f\mid(W\times W)$ 非退化和 $u\in W$，有 $u=0$；因此 $W\cap W^\perp=\{0\}$. 如果 $v\in V$，则 $f(\ \ ,v)\mid W$ 是 W 上的线性泛函；即 $f(\ \ ,v)\mid W\in W^*$. 根据系 9.75，存在 $w_0\in W$ 使得对一切 $w\in W$ 有 $f(w,v)=f(w,w_0)$. 因此，$v=w_0+(v-w_0)$，其中 $w_0\in W$ 和 $v-w_0\in W^\perp$. ■

命题中的直和分解有一个名称.

定义 如果(V,f)是内积空间，则我们说直和

$$V=W_1\oplus\cdots\oplus W_r$$

[700] 是一个**正交直和**，如果对一切 $w_i\in W_i$ 和 $w_j\in W_j$，其中 $i\neq j$，有 $f(w_i,w_j)=0$.

现在我们更仔细地观察特殊双线性型；先考察交错型，然后考察对称型.

我们先构造域 k 上的二维向量空间 V 上的一切交错双线性型 f. $f=0$ 总是一例. 除此之外，存在两个向量 e_1, $e_2\in V$ 使得 $f(e_1,e_2)\neq 0$；比如 $f(e_1,e_2)=c$. 如果把 e_1 换成 $e_1'=c^{-1}e_1$，则 $f(e_1',e_2)=1$. 因 f 是交错的，f 关于基 e_1'，e_2 的内积矩阵 A 是 $A=\begin{bmatrix}0&1\\-1&0\end{bmatrix}$.

定义 域 k 上的一个**双曲平面**是指 k 上的一个二维向量空间，它配置了非零交错双线性型.

刚才已经看到在二维交错空间(V,f)中，f 不恒为零就有一个内积矩阵 $A=\begin{bmatrix}0&1\\-1&0\end{bmatrix}$.

定理 9.78 设(V,f)是交错空间，其中 V 是域 k 上的向量空间. 如果 f 非退化，则存在正交直和

$$V=H_1\oplus\cdots\oplus H_m,$$

其中每个 H_i 是双曲平面.

证明 对 $\dim(V)\geqslant 1$ 用归纳法证明. 关于基础步，注意一维空间上的交错型必是 0，因此退化，所以 $\dim(V)\geqslant 2$. 如果 $\dim(V)=2$，则我们已经看到 V 是一个双曲平面. 关于归纳步，注意存在向量 $e_1,e_2\in V$ 使得 $f(e_1,e_2)\neq 0$（因为 f 非退化，因此非零），而且可以把它正规化从而使得 $f(e_1,e_2)=1$；如果 $f(e_1,e_2)=d$，把 e_2 换成 $d^{-1}e_2$ 即可. 子空间 $H_1=\langle e_1,\ e_2\rangle$是双曲平面，且限制 $f\mid(H_1\times H_1)$ 非退化. 于是命题 9.77 给出 $V=H_1\oplus H_1^\perp$. 根据习题 9.56，因 f 到 $H_1^\perp$ 的

限制是非退化的，所以运用归纳假设可得结果. ■

系 9.79 设 (V,f) 是交错空间，其中 V 是域 k 上的向量空间. 如果 f 是非退化的，则 $\dim(V)$ 是偶数.

证明 根据定理，V 是二维子空间的直和. ■

定义 设 (V,f) 是交错空间，其中 f 非退化. 一个辛[⊖]基是指基 $x_1,y_1,\cdots,x_m,y_m$ 满足对一切 i，$f(x_i,y_i)=1, f(y_i,x_i)=-1$，且其他一切 $f(x_i,x_j), f(y_i,y_j), f(x_i,y_j)$ 和 $f(y_j,x_i)$ 都是 0.

系 9.80 设 (V,f) 是交错空间，其中 f 非退化，[⊜]并设 A 是 f（关于 V 的某个基）的内积矩阵. 701

（i）存在 V 的辛基 $x_1,y_1,\cdots,x_m,y_m$，且 A 是 $2m\times 2m$ 矩阵，其中 m 是某个 $\geqslant 1$ 的数.

（ii）A 和形如 $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ 的块的矩阵直和相合，且这个矩阵直和与 $\begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}$ 相合，其中 I 是 $m\times m$ 单位矩阵.

（iii）每个域 k 上的非奇异反称矩阵 A 相合于 2×2 块 $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ 的直和.

证明 （i）根据定理 9.78，存在辛基，因此 V 是偶数维的.

（ii）内积矩阵 A 和关于辛基 $x_1,y_1,\cdots,x_m,y_m$ 的内积矩阵相合. 把辛基重排成 $x_1,\cdots,x_m,y_1,\cdots,y_m$，得到另一个相合的内积矩阵.

（iii）经简单计算可得. ■

定义 设 (V,f) 是对称空间，并设 $E=e_1,\cdots,e_n$ 是 V 的基. 如果对一切 $i\neq j$ 有 $f(e_i,e_j)=0$，则称 E 为**正交基**. 如果 $f(e_i,e_j)=\delta_{ij}$，其中 δ_{ij} 是克罗内克 δ，则称 E 为**规范正交基**.

如果 $e_1,\cdots,e_n$ 是对称空间 (V,f) 的正交基，则 $V=\langle e_1\rangle\oplus\cdots\oplus\langle e_n\rangle$ 是正交直和. 在系 9.76 中我们看到，如果 (V,f) 是对称空间且 f 非退化，又如果 $e_1,\cdots,e_n$ 是 V 的基，则存在 V 的基 $b_1,\cdots,b_n$ 使得 $f(e_i,b_j)=\delta_{ij}$. 如果 E 是规范正交基，则可以对一切 i 令 $b_i=e_i$.

定理 9.81 设 (V,f) 是对称空间，其中 V 是特征不为 2 的域 k 上的向量空间.

（i）V 有正交基，由此元素在 k 中的每个对称矩阵 A 和一个对角矩阵相合.

（ii）如果 $C=\mathrm{diag}[c_1^2d_1,\cdots,c_n^2d_n]$，则 C 和 $D=\mathrm{diag}[d_1,\cdots,d_n]$ 相合.

（iii）如果 f 是非退化的，且 k 中的每个元素在 k 中有平方根，则 V 有规范正交基. 元素在 k 中的每个非奇异对称矩阵 A 和 I 相合. 702

证明 （i）如果 $f=0$，则每个基都是正交基. 现在可以假定 $f\neq 0$. 因为 k 的特征不为 2，可以运用习题 9.54，由此存在某个 $v\in V$ 使得 $f(v,v)\neq 0$（否则，f 既是对称的又是交错的）. 如果 $W=\langle v\rangle$，则 $f\mid(W\times W)$ 是非退化的，从而命题 9.77 给出 $V=W\oplus W^{\perp}$. 对 $\dim(V)$ 用归纳法可以完成证明.

⊖ 术语辛（symplectic）由外尔（H. Weyl）首先使用. 在他的书《The Classical Groups: Their Invariants and Representations》165 页上，他写道："我以前提出的名词'复群（complex group）'是为了针对线聚，那是由消失反对称双线性型定义的，但这个名词变得越来越麻烦，因为字'complex'和复数的涵义相冲突. 所以我提出把它换成相应的希腊形容词'辛（symplectic）'. 迪克森把这种群称为'阿贝尔线性群'，以纪念第一个研究它的阿贝尔."

⊜ 如果型 f 退化，则 A 和几个 2×2 块 $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ 与几个 0 块的直和相合.

如果 A 是 $n\times n$ 对称矩阵，则命题9.70(i)表明存在对称双线性型 f 和基 $U=u_1,\cdots,u_n$ 使得 A 是 f 关于 U 的内积矩阵. 刚才已经看到存在正交基 $v_1,\cdots,v_n$，从而命题9.70(iii)表明 A 和对角矩阵 $\mathrm{diag}[f(v_1,v_1),\cdots,f(v_n,v_n)]$ 相合.

(ii) 如果一个正交基由向量 v_i 组成，且满足 $f(v_i,v_i)=c_i^2d_i$，则把每个 v_i 换成 $v_i'=c_i^{-1}v_i$ 得正交基满足 $f(v_i',v_i')=d_i$. 由此，f 关于基 $v_1',\cdots,v_n'$ 的内积矩阵是 $D=\mathrm{diag}[d_1,\cdots,d_n]$.

(iii) 根据 (i)，存在正交基 $v_1,\cdots,v_n$；对每个 i，设 $f(v_i,v_i)=c_i$. 因 f 非退化，对一切 i 有 $c_i\neq0$ (关于这个正交基的内积矩阵的行列式是 $c_1c_2\cdots c_n$)；根据假设，因每个 c_i 都是一个平方数，我们可以和 (ii) 一样把每个 v_i 换成 $v_i'=(\sqrt{c_i})^{-1}v_i$；这个新基是规范正交的. 因为关于规范正交基的内积矩阵是单位矩阵 I，所以最后一个陈述成立. ■

注意，定理 9.81 没有说特征不为 2 的域 k 上的任两个对角矩阵相合；这要依赖于 k. 例如，如果 $k=\mathbb{C}$，则一切 (非奇异) 对角矩阵和 I 相合，但我们现在证明，如果 $k=\mathbb{R}$，则结论不成立.

定义 如果$\mathbb{R}$上的向量空间 V 上的对称双线性型 f 对一切非零 $v\in V$ 有 $f(v,v)>0$，则称 f 是**正定的**. 如果对一切非零 $v\in V$ 有 $f(v,v)<0$，则称 f 是**负定的**.

下一结果和它的矩阵推论由西尔维斯特 (J. J. Sylvester) 证明. 当 $n=2$ 时，它对圆锥截线进行了分类，当 $n=3$ 时，对二次曲面进行了分类.

引理 9.82 如果 f 是$\mathbb{R}$上的 m 维向量空间 V 上的对称双线性型，则存在正交直和

$$V=W_+\oplus W_-\oplus W_0,$$

其中 $f\mid W_+$ 是正定的，$f\mid W_-$ 是负定的，$f\mid W_0$ 恒为 0. 此外，这三个子空间的维数由 f 唯一确定.

证明 根据定理 9.81，存在 V 的正交基 $v_1,\cdots,v_m$. 记 $f(v_i,v_i)$为 d_i. 和任意实数一样，每个 d_i 或者是正的，或者是负的，或者是 0，我们重新排列基向量，使得 $v_1,\cdots,v_p$ 有正的 d_i，$v_{p+1},\cdots,v_{p+r}$有负的 d_i，剩下的向量有 $d_i=0$. 易知 V 是正交直和

703

$$V=\langle v_1,\cdots,v_p\rangle\oplus\langle v_{p+1},\cdots,v_{p+r}\rangle\oplus\langle v_{p+r+1},\cdots,v_m\rangle,$$

且 f 到各个直和项的限制是正定的、负定的和零.

现在 $W_0=V^\perp$ 只依赖于 f，因此它的维数也只依赖于 f. 为证明另外两个维数的唯一性，假设存在另一个正交直和 $V=W'_+\oplus W'_-\oplus W_0$. 如果 $T:V\to W_+$ 是投射，则 $\ker T=W_-\oplus W_0$. 由此，如果 $\varphi=T\mid W'_+$，则

$$\ker\varphi=W'_+\cap\ker T=W'_+\cap(W_-\oplus W_0).$$

然而，如果 $v\in W'_+$，则 $f(v,v)\geqslant0$，而如果 $v\in W_-\oplus W_0$，则 $f(v,v)\leqslant0$；因此，如果 $v\in\ker\varphi$, 则 $f(v,v)=0$. 但根据 W'_+ 的定义，$f\mid W'_+$ 是正定的，从而 $f(v,v)=0$ 蕴涵 $v=0$. 由此可知 $\ker\varphi=\{0\}$，且推出 $W'_+\to W_+$ 是单射；所以，$\dim(W'_+)\leqslant\dim(W_+)$. 反过来的不等式可类似得到证明，因此 $\dim(W'_+)=\dim(W_+)$. 最后，公式 $\dim(W_-)=\dim(V)-\dim(W_+)-\dim(W_0)$ 和带撇的同样的公式给出 $\dim(W'_-)=\dim(W_-)$. ■

定理 9.83 (惯性定律) $\mathbb{R}$上的每个 $n\times n$ 对称矩阵 A 和形如

$$\begin{bmatrix}I_p & 0 & 0\\ 0 & -I_r & 0\\ 0 & 0 & 0\end{bmatrix}$$

的矩阵相合．此外，f 的符号差 $s=p-r$ 是合理定义的，且两个 $n\times n$ 实对称矩阵相合当且仅当它们有相同的秩和相同的符号差．

证明 根据定理 9.81，A 和对角矩阵 $\mathrm{diag}[d_1,\cdots,d_n]$ 相合，其中 $d_1,\cdots,d_p$ 是正的，$d_{p+1},\cdots,d_{p+r}$ 是负的，$d_{p+r+1},\cdots,d_n$ 是 0．但每个正实数都是平方数，而每个负实数都是负的平方数；现在由定理 9.81（ⅱ），A 和定理陈述中的矩阵相合．

显然相合的 $n\times n$ 矩阵有相同的秩和相同的符号差．反之，设 A 和 A' 有相同的秩和相同的符号差．现在 A 与矩阵直和 $I_p\oplus -I_r\oplus 0$ 相合，A' 与 $I_{p'}\oplus -I_{r'}\oplus 0$ 相合．因 $\mathrm{rank}(A)=\mathrm{rank}(A')$，有 $p'+r'=p+r$；因符号差相同，有 $p'-r'=p-r$．由此，$p'=p$ 和 $r'=r$，所以 A 和 A' 都相合于同一个有若干 1、若干 −1 和若干 0 的对角矩阵，因此彼此相合． ■

如果一个 f 非退化的对称空间 (V,f) 恒有规范正交基，即每个对称矩阵都和单位矩阵相合，那么这种情形是最简单的．但情况并非如此，例如实 2×2 矩阵 $-I$ 和 I 的符号差不同（I 的符号差是 2，$-I$ 的符号差是 −2)，所以它们不相合．

和双线性型密切相关的是二次型；对定义在域 k 上的向量空间 V 上的双线性型 f，考虑由 $Q(v)=f(v,v)$ 给出的函数 $Q:V\to k$，由此引出二次型．

704

定义 设 V 是域 k 上的向量空间．**二次型**是指函数 $Q:V\to k$ 满足

（ⅰ）对一切 $v\in V$ 和 $c\in k$ 有 $Q(cv)=c^2Q(v)$；

（ⅱ）由

$$g(u,v)=Q(u+v)-Q(u)-Q(v)$$

定义的函数 $g:V\times V\to k$ 是双线性型．

例 9.84 （ⅰ）如果 f 是向量空间 V 上的双线性型，对一切 $v\in V$ 定义 $Q(v)=f(v,v)$；我们证明 Q 是二次型．现在 $Q(cv)=f(cv,cv)=c^2f(v,v)=c^2Q(v)$，给出定义中的第一个公理．如果 u，$v\in V$，则

$$\begin{aligned}Q(u+v)&=f(u+v,u+v)\\&=f(u,u)+f(u,v)+f(v,u)+f(v,v)\\&=Q(u)+Q(v)+g(u,v),\end{aligned}$$

其中

$$g(u,v)=f(u,v)+f(v,u).$$

容易验证 g 是对称双线性型．

（ⅱ）刚才已经看到每个双线性型 f 确定一个二次型 Q．如果 f 是对称的且 k 的特征不为 2，则 Q 确定 f．事实上，此时公式 $2f(u,v)=g(u,v)$ 给出 $f(u,v)=\frac{1}{2}g(u,v)$．

（ⅲ）如果 f 是定义在 $\mathbb{R}^n$ 上的通常的点积，则对应的二次型是 $Q(v)=\|v\|^2$，其中 $\|v\|$ 是向量 v 的长度．

（ⅳ）如果 f 是向量空间 V 上的双线性型，关于某个基 $e_1,\cdots,e_n$ 的内积矩阵是 $A=[a_{ij}]$，如果 $u=\sum_i c_ie_i$，则

$$Q(u)=\sum_{i,j}a_{ij}c_ic_j.$$

例如，如果 $n=2$，则有

$$Q(u) = a_{11}c_1^2 + (a_{12} + a_{21})c_1c_2 + a_{22}c_2^2.$$

于是，二次型其实就是二次齐次多项式. ■

我们刚才在上面的例子中已经看到，如果 k 的特征不为 2，则对称双线性型和二次型不过是用两种不同的方法看待同一事物，这是因为其中一个确定另一个.

705

我们已经对$\mathbb{C}$和$\mathbb{R}$上的二次型 Q 进行了分类. 有限域上和素域上的分类也已经知道，现在陈述（不证明）当 Q 非退化时的结果. 给定一个定义在域 k 上的有限维向量空间 V 上的二次型 Q，它的相伴双线性型是

$$f(x,y) = Q(x+y) - Q(x) - Q(y).$$

如果两个二次型的相伴双线性型有相合的内积矩阵，则称这两个二次型**等价**，如果一个二次型的双线性型非退化，则称这个二次型**非退化**. 正如刚才在例 9.84 中看到的，f 是对称双线性型（当 k 的特征不为 2 时，f 由 Q 唯一确定）. 如果 k 是有奇数特征的有限域，则 k 上的两个非退化二次型等价当且仅当它们有相同的判别式（见 Kaplansky 所著的《Linear Algebra and Geometry; A Second Course》14～15 页）. 如果 k 是特征为 2 的有限域，则相应的理论稍微复杂一点. 此时，相伴对称双线性型

$$g(x,y) = Q(x+y) + Q(x) + Q(y)$$

必是交错的，这是因为 $g(x,x) = Q(2x) + 2Q(x) = 0$. 所以，$V$ 有辛基 x_1，y_1，…，x_m，y_m. 定义 Q 的**阿尔夫（Arf）不变量**为

$$\mathrm{Arf}(Q) = \sum_{i=1}^{m} Q(x_i)Q(y_i)$$

[Arf 不变量是一个不变量并不是显而易见的；即 Arf(Q)不依赖于辛基的选取；一个极好的证明见 R. L. Dye, "On the Arf Invariant," Journal of Algebra53 (1978)，36～39 页]. 如果 k 是特征为 2 的有限域，则 k 上的两个非退化二次型等价当且仅当它们有相同的判别式和相同的 Arf 不变量（见 Kaplansky 所著的《Linear Algebra and Geometry; A Second Course》，27～33 页）. $\mathbb{Q}$ 上二次型的分类难度更大（见 Borevich 和 Shafarevich 所著的《Number Theory》，61～70 页）. 正如$\mathbb{R}$能够借助通常的度量 $d(a,b) = |a-b|$ 把$\mathbb{Q}$完备化而得到（即加进一些点迫使柯西序列收敛），对每个素数 p，我们也可以根据 p-进位度量把$\mathbb{Z}$完备化（见 503 页的讨论）. 完备化$\mathbb{Z}_p$ 叫做 **p-进位整数**. $\mathbb{Z}$ 上的 p-进位度量可以扩张到$\mathbb{Q}$，它的完备化$\mathbb{Q}_p$[它是 Frac($\mathbb{Z}_p$)] 叫做 **p-进位数**. **哈塞-闵可夫斯基**（Hasse-Minkowski）**定理**说，$\mathbb{Q}$ 上的两个二次型等价当且仅当它们在$\mathbb{R}$上等价，且对一切素数 p 在$\mathbb{Q}_p$ 上等价.

线性代数最初的一些定理考虑了向量空间的结构，这是为了给线性变换的讨论铺平道路. 类似地，内积空间最初的一些定理使我们能够讨论相应的线性变换.

定义 如果(V,f)是内积空间，其中 V 是域 k 上的有限维向量空间，f 是非退化双线性型，则一个**等距同构**是指一个线性变换 $\varphi: V \to V$，使得对一切 $u,v \in V$，

706

$$f(u,v) = f(\varphi u, \varphi v).$$

命题 9.85 设(V,f)是内积空间，其中 f 是非退化双线性型，设 $E = e_1,\cdots,e_n$ 是 V 的基，并设 A 是关于 E 的内积矩阵. 则 $\varphi \in \mathrm{GL}(V)$ 是等距同构当且仅当它的矩阵 $M = {}_E[\varphi]_E$ 满足等式 $M^tAM = A$.

证明 回忆等式

$$f(b,c) = B^tAC,$$

其中 $b,c \in V$ 和 $B,C \in k^n$ 是它们关于基 E 的坐标向量. 令 E_1，…，E_n 是 k^n 的标准基. 因为 ME_i

是 M 的第 i 列，它是 $\varphi(e_i)$的坐标向量，从而对一切 i 有

$$\varphi(e_i) = ME_i,$$

所以，

$$f(\varphi e_i, \varphi e_j) = (ME_i)^t A(ME_j) = E_i^t(M^tAM)E_j.$$

如果 φ 是等距同构，则

$$f(\varphi e_i, \varphi e_j) = f(e_i, e_j) = E_i^tAE_j,$$

从而 $f(e_i,e_j) = E_i^tAE_j = E_i^t(M^tAM)E_j$. 因此，命题 9.70(ⅱ) 给出 $M^tAM = A$.

反之，如果 $M^tAM = A$，则

$$f(\varphi e_i, \varphi e_j) = E_i^t(M^tAM)E_j = E_i^tAE_j = f(e_i, e_j),$$

因此 φ 是等距同构. ■

命题 9.86 设(V,f)是内积空间，其中 V 是域 k 上的有限维向量空间，f 是非退化双线性型. 则 $\mathrm{Isom}(V,f)$，即(V,f)的一切等距同构的集合是 $\mathrm{GL}(V)$的子群.

证明 我们证明 $\mathrm{Isom}(V,f)$是子群；当然，1_V 是等距同构. 设 $\varphi: V\to V$ 是等距同构. 如果 $u\in V$ 和 $\varphi u=0$，则对一切 $v\in V$，有

$$0 = f(\varphi u, \varphi v) = f(u,v).$$

因 f 非退化，$u=0$ 和 φ 是单射. 因此，$\dim(\mathrm{im}\varphi) = \dim(V)$ ，从而根据 3.90(ⅱ),$\mathrm{im}\varphi = V$. 所以每个等距同构都是非奇异的 .

等距同构 φ 的逆也是等距同构：对一切 u，$v\in V$，

$$\begin{aligned} f(\varphi^{-1}u, \varphi^{-1}v) &= f(\varphi\varphi^{-1}u, \varphi\varphi^{-1}v) \\ &= f(u,v). \end{aligned}$$

最后，两个等距同构 φ 和 θ 的复合也是等距同构：

$$f(u,v) = f(\varphi u, \varphi v) = f(\theta\varphi u, \theta\varphi v).$$ ■

计算一般非奇异矩阵的逆是十分费事的，但计算等距同构的逆则容易得多 . [707]

定义 设 (V,f) 是内积空间，它的双线性型 f 非退化. 线性变换 $T: V\to V$ 的**伴随线性变换**是指线性变换 $T^*: V\to V$，满足对一切 $u,v\in V$，

$$f(Tu,v) = f(u, T^*v).$$

我们来看伴随线性变换的存在性.

命题 9.87 如果(V,f)是内积空间，它的双线性型 f 非退化，则每个线性变换 $T: V\to V$ 都有伴随线性变换.

证明 设 e_1，…，e_n 是 V 的基. 对每个 j，易知由

$$\varphi_j(v) = f(Tv, e_j)$$

定义的函数 $\varphi_j: V\to k$ 是一个线性泛函. 根据系 9.75，存在 $u_j\in V$ 使得对一切 $v\in V$ 有 $\varphi_j(v) = f(v,u_j)$. 定义 $T^*: V\to V$ 为 $T^*(e_j) = u_j$ ，并注意

$$f(Te_i, e_j) = \varphi_j(e_i) = f(e_i, u_j) = f(e_i, T^*e_j).$$ ■

命题 9.88 设(V,f)是内积空间，它的双线性型 f 非退化. 如果 $T: V\to V$ 是有伴随线性变换 T^* 的线性变换，则 T 是等距同构当且仅当 $T^*T = 1_V$ ，此时，$T^* = T^{-1}$.

证明 如果 $T^*T = 1_V$，则对一切 u，$v\in V$ 有

$$f(Tu, Tv) = f(u, T^*Tv) = f(u,v),$$

因此 T 是等距同构.

反之，假定 T 是等距同构. 选取 $v\in V$；对一切 $u\in V$ 有

$$\begin{aligned} f(u,T^*Tv-v) &= f(u,T^*Tv)-f(u,v) \\ &= f(Tu,Tv)-f(u,v) \\ &= 0. \end{aligned}$$

因 f 非退化，$T^*Tv-v=0$；即 $T^*Tv=v$. 因为这对一切 $v\in V$ 成立，所以 $T^*T=1_V$. ■

定义 设(V,f)是内积空间，其中 V 是域 k 上的有限维向量空间，f 是非退化双线性型.

（ⅰ）如果 f 是交错的，则称 $\mathrm{Isom}(V,f)$ 为**辛群**，记为 $\mathrm{Sp}(V,f)$.

708

（ⅱ）如果 f 是对称的，则称 $\mathrm{Isom}(V,f)$ 为**正交群**，记为 $O(V,f)$.

选定域 k 上 n 维向量空间 V 的一个基 E，总有同构 μ：$\mathrm{GL}(V)\to\mathrm{GL}(n,k)$，$\mathrm{GL}(n,k)$ 是 k 上一切 $n\times n$ 非奇异矩阵的群. 特别地，设 (V,f) 是 f 非退化的交错空间，并设 $E=x_1,y_1,\cdots,x_m,y_m$ 是 V 的辛基（根据系 9.80，辛基存在）；回忆 $n=\dim(V)$ 是偶数. 记 $\mathrm{Sp}(V,f)$ 的象为 $\mathrm{Sp}(2m,k)$. 类似地，如果(V,f)是 f 非退化的对称空间，E 是正交基（根据定理 9.81，当 k 的特征不为 2 时，正交基存在），记 $O(V,f)$的象为 $O(n,f)$.

我们求对称的或交错的双线性型的伴随.

命题 9.89 设(V,f)是对称空间，其中 V 是域 k 上的 n 维向量空间，f 是非退化的，并设$E=e_1,\cdots,e_n$ 是有 $f(e_i,e_i)=c_i$ 的正交基.

如果 $B=[b_{ij}]$是关于 E 的矩阵，则它的伴随矩阵 B^* 是它的“加权”转置 $[c_i^{-1}c_jb_{ji}]$. 特别地，如果 E 是规范正交基，则 $B^*=B^t$，B^t 是 B 的转置.

注 由此，B 是正交的当且仅当 $B^tB=I$.

证明 我们有

$$\begin{aligned} f(Be_i,e_j) &= f\Big(\sum_\ell b_{\ell i}e_\ell,e_j\Big) \\ &= \sum_\ell b_{\ell i}f(e_\ell,e_j) \\ &= b_{ji}c_j. \end{aligned}$$

如果 $B^*=[b_{ij}^*]$，则经类似的计算得

$$f(e_i,B^*e_j)=\sum b_{\ell j}^*f(e_i,e_\ell)=c_ib_{ij}^*.$$

因 $f(Be_i,e_j)=f(e_i,B^*e_j)$，对一切 i,j 有

$$b_{ji}c_j=c_ib_{ij}^*.$$

因 f 非退化，所以一切 $c_i\neq 0$，从而

$$b_{ij}^*=c_i^{-1}c_jb_{ji}.$$

如果 E 是正交基，则对一切 i 有 $c_i=1$，由此得最后的注记. ■

709

如何识别辛矩阵？

命题 9.90 设(V,f)是交错空间，其中 V 是域 k 上的 $2m$ 维向量空间，f 是非退化的，并设 E 是排列为 $x_1,\cdots,x_m,y_1,\cdots,y_m$ 的辛基.

关于 E 的划分为 $m\times m$ 块的矩阵 $B=\begin{bmatrix}P & Q\\ S & T\end{bmatrix}$的伴随是

$$B^* = \begin{bmatrix} T^t & -Q^t \\ -S^t & P^t \end{bmatrix}.$$

注 由此，$B \in \mathrm{Sp}(2m,k)$ 当且仅当 $B^* B = I$.

证明 因为对一切 $i,j, f(x_\ell, x_j) = 0$ 和 $f(y_\ell, x_j) = -\delta_{\ell j}$，所以有

$$\begin{aligned} f(Bx_i, x_j) &= f\Big(\sum_\ell p_{\ell i} x_\ell + s_{\ell i} y_\ell, x_j\Big) \\ &= \sum_\ell p_{\ell i} f(x_\ell, x_j) + \sum_\ell s_{\ell i} f(y_\ell, x_j) \\ &= -s_{ji}, \end{aligned}$$

把伴随矩阵 B^* 划分为 $m \times m$ 块：

$$B^* = \begin{bmatrix} \Pi & K \\ \Sigma & \Omega \end{bmatrix}.$$

由于 $f(x_i, x_\ell) = 0$ 和 $f(x_i, y_\ell) = \delta_{i\ell}$，因此

$$\begin{aligned} f(x_i, B^* x_j) &= f\Big(x_i, \sum_\ell \pi_{\ell j} x_\ell + \sigma_{\ell j} y_\ell\Big) \\ &= \sum_\ell \pi_{\ell j} f(x_i, x_\ell) + \sum_\ell \sigma_{\ell j} f(x_i, y_\ell) \\ &= \sigma_{ij}. \end{aligned}$$

因 $f(Bx_i, x_j) = f(x_i, B^* x_j)$，有 $\sigma_{ij} = -s_{ji}$. 因此，$\Sigma = -S^t$. 可类似计算 B^* 的另外的块. ■

下一个问题是 $\mathrm{Isom}(V,f)$ 是否依赖于非退化交错双线性型 f 的选取. 考虑 $\mathrm{GL}(V)$ 作用在一切函数 $V \times V \to k$ 的集合 $k^{V \times V}$ 上：如果 $f: V \times V \to k$ 和 $\varphi \in \mathrm{GL}(V)$，则定义 $\varphi f = f^\varphi$，其中

$$f^\varphi(b,c) = f(\varphi^{-1} b, \varphi^{-1} c).$$

这个公式确实产生一个作用：如果 $\theta \in \mathrm{GL}(V)$，则 $(\varphi\theta) f = f^{\varphi\theta}$，其中

$$\begin{aligned} (\varphi\theta) f(b,c) &= f^{\varphi\theta}(b,c) \\ &= f((\varphi\theta)^{-1} b, (\varphi\theta)^{-1} c) \\ &= f(\theta^{-1} \varphi^{-1} b, \theta^{-1} \varphi^{-1} c). \end{aligned}$$

710

另一方面，$\varphi(\theta f)$ 定义为

$$\begin{aligned} (f^\theta)^\varphi(b,c) &= f^\theta(\varphi^{-1} b, \varphi^{-1} c) \\ &= f(\theta^{-1} \varphi^{-1} b, \theta^{-1} \varphi^{-1} c), \end{aligned}$$

因此，$(\varphi\theta) f = \varphi(\theta f)$.

定义 设 V 和 W 都是域 k 上的有限维向量空间，并设 $f: V \times V \to k$ 和 $g: W \times W \to k$ 都是双线性型. 如果存在等距同构 $\varphi: V \to W$，则称 f 和 g **等价**.

命题 9.91 如果 V 是域 k 上的有限维向量空间，f，$g: V \times V \to k$ 都是双线性型，则下列陈述等价.

(i) f 和 g 等价.

(ii) 如果 $E = e_1, \cdots, e_n$ 是 V 的基，则 f 和 g 关于 E 的内积矩阵相合.

(iii) 存在 $\varphi \in \mathrm{GL}(V)$ 使得 $g = f^\varphi$.

证明 (i) ⇒ (ii). 如果 $\varphi: V \to V$ 是等距同构，则对一切 $b, c \in V, g(\varphi(b), \varphi(c)) = f(b,c)$. 如果 $E = e_1, \cdots, e_n$ 是 V 的基，则因为 φ 是同构，所以 $E' = \varphi(e_1), \cdots, \varphi(e_n)$ 也是基. 因此对一切 i,j，$A' = [g(\varphi(e_i), \varphi(e_j))] = [f(e_i, e_j)] = A$；即 g 关于 E' 的内积矩阵 A' 等于 f 关于 E 的内积矩阵 A. 根据命题9.70(iii)，g 关于 E 的内积矩阵 A'' 和 A 相合.

（ⅱ）⇒（ⅲ）. 如果 $A=[f(e_i,e_j)]$ 和 $A'=[g(e_i,e_j)]$，则存在非奇异矩阵 $Q=[q_{ij}]$ 使得 $A'=Q^tAQ$. 定义 $\theta: V\to V$ 为满足 $\theta(e_j)=\sum_\nu q_{\nu j}e_\nu$ 的线性变换. 最后，$g=f^{\theta^{-1}}$：

$$[g(e_i,e_j)]=A'=Q^tAQ=\Big[f\Big(\sum_\nu q_{\nu i}e_\nu,\sum_\lambda q_{\lambda j}e_\lambda\Big)\Big]$$
$$=[f(\theta(e_i),\theta(e_j))]=[f^{\theta-1}(e_i,e_j)].$$

（ⅲ）⇒（ⅰ）. 由定义显然 $\varphi^{-1}:(V,g)\to(V,f)$ 是等距同构：

$$g(b,c)=f^\varphi(b,c)=f(\varphi^{-1}b,\varphi^{-1}c).$$

所以 g 和 f 等价. ■

命题 9.92 （ⅰ）设 (V,f) 是内积空间，其中 V 是域 k 上的有限维向量空间和 f 是非退化双线性型. f 作用在 $k^{V\times V}$ 上的稳定化子 $\mathrm{GL}(V)_f$ 是 $\mathrm{Isom}(V,f)$.

（ⅱ）如果 $g: V\times V\to k$ 位于 f 的同一轨道中，则 $\mathrm{Isom}(V,f)$ 和 $\mathrm{Isom}(V,g)$ 同构；事实上，它们是 $\mathrm{GL}(V)$ 的共轭子群.

711

证明 （ⅰ）根据稳定化子的定义，$\varphi\in\mathrm{GL}(V)_f$ 当且仅当 $f^\varphi=f$；即对一切 $b,c\in V$，有 $f(\varphi^{-1}b,\varphi^{-1}c)=f(b,c)$. 于是，$\varphi^{-1}$，因而 φ 是等距同构.

（ⅱ）根据习题 2.99，有某个 $\tau\in\mathrm{GL}(V)$ 使得 $\mathrm{GL}(V)_g=\tau(\mathrm{GL}(V)_f)\tau^{-1}$；即 $\mathrm{Isom}(V,g)=\tau\mathrm{Isom}(V,f)\tau^{-1}$. ■

由命题 9.92，等价双线性型有同构的等距同构群. 我们现在能够证明如不计同构辛群不依赖于非退化交错型的选取.

定理 9.93 如果 (V,f) 和 (V,g) 都是交错空间，其中 f 和 g 都是非退化的，则 f 和 g 等价且

$$\mathrm{Sp}(V,f)\cong\mathrm{Sp}(V,g).$$

证明 根据系9.80(ⅱ)，任意非退化交错双线性型的内积矩阵和 $\begin{bmatrix}0 & I\\ -I & 0\end{bmatrix}$ 相合，其中 I 是单位矩阵. 现在结果由命题 9.91 可得. ■

辛群引出单群. 如果 k 是域，定义 $\mathrm{PSp}(2m,k)=\mathrm{Sp}(2m,k)/Z(2m,k)$，其中 $Z(2m,k)$ 是 $\mathrm{Sp}(2m,k)$ 中一切标量矩阵组成的子群. 群 $\mathrm{PSp}(2m,k)$ 对一切 $m\geqslant1$ 和一切域 k 除了三个例外都是单群，这三个例外是：$\mathrm{PSp}(2,\mathbb{F}_2)\cong S_3$，$\mathrm{PSp}(2,\mathbb{F}_3)\cong A_4$ 和 $\mathrm{PSp}(4,\mathbb{F}_2)\cong S_6$.

正交群，即 f 非退化的对称空间 (V,f) 的等距同构群也引出单群. 然而和辛群相比，它们依赖于域 k 的性质. 我们把注意力限制在有限域 k. k 有奇数特征和 k 有特征 2 的情形必须分别考虑，在每种情形下还必须考虑 $\dim(V)$ 是奇数还是偶数. 如果 k 有奇数特征 p，当 n 是奇数时，只有一个正交群 $O(n,p^m)$ ⊖，而当 n 是偶数时有两个，即 $O^+(n,p^m)$ 和 $O^-(n,p^m)$. 它们引出的单群定义如下：首先，构成 $SO^\varepsilon(n,p^m)$，它是行列式为 1 的一切正交矩阵（其中 $\varepsilon=+$ 或 $\varepsilon=-$）；然后除以 $SO^\varepsilon(n,p^m)$ 中一切标量矩阵以构成 $PSO^\varepsilon(n,p^m)$. 最后，可以定义 $PSO^\varepsilon(n,p^m)$ 的子群 $\Omega^\varepsilon(n,p^m)$（本质上是换位子群），这些群是单的，除了有限个例外（可以明确地列出）.

当 k 有特征 2 时，我们常从一个二次型出发而不是对称双线性型. 此时，当 n 是奇数时，也只有一个正交群 $O(n,2^m)$，但 n 是偶数时有两个，记为 $O^+(n,2^m)$ 和 $O^-(n,2^m)$. 如果 n 是奇数，比如

⊖ 当 k 是有限域时，比如 $k=\mathbb{F}_q$，其中 q 是某个素数幂，我们常把 $\mathrm{GL}(n,k)$ 记为 $\mathrm{GL}(n,q)$. 对于 $\mathrm{GL}(n,k)$ 形成的任意矩阵群也有类似的记法.

$n=2\ell+1$，则 $O(2\ell+1,2^m)\cong \mathrm{Sp}(2\ell,2^m)$，因此只需考虑偶数维对称空间形成的正交群 $O^\epsilon(2\ell,2^m)$。这些群中的每一个用类似于奇数特征的状况的方式引出一个单群. 详情参考 E. Artin 的书《Geometric Algebra》；Conway 等的《Atlas of Finite Groups》；J. Dieudonné 的《La Géometrie des Groupes Classiques》；M. Suzuki 的《Group Theory I》以及 Kostrikin－Shafarevich 的《Algebra IX》中 Carter 的论文. 712

二次型在数论中尤其重要. 对于这个主题的介绍见 Hahn 的《Quadratic Algebras, Clifford Algebras, and Arithmetic Witt Groups》；Lam 的《The Algebraic Theory of Quadratic Forms》；以及 O'Meara 的《Introduction to Quadratic Forms》.

习题

9.51 在解析几何中证明了如果 ℓ_1 和 ℓ_2 是斜率分别为 m_1 和 m_2 的直线，则 ℓ_1 和 ℓ_2 垂直当且仅当 $m_1m_2=-1$. 如果

$$\ell_i=\{\alpha v_i+u_i:\alpha\in\mathbb{R}\},$$

其中 $i=1,2$，证明 $m_1m_2=-1$ 当且仅当点积 $v_1\cdot v_2=0$.（因两条直线都有斜率，它们都不是垂线.）

提示：向量 $v=(a,b)$ 的斜率是 $m=b/a$.

9.52 (i) 在微积分中，在空间中过点 u 的直线定义为

$$\{u+\alpha w:\alpha\in\mathbb{R}\}\subseteq\mathbb{R}^3,$$

其中 w 是固定的非零向量. 证明过原点的每条直线都是 $\mathbb{R}^3$ 的一个一维子空间.

(ii) 在微积分中，在空间中过点 u 的平面定义为子集

$$\{v\in\mathbb{R}^3:(v-u)\cdot n=0\}\subseteq\mathbb{R}^3,$$

其中 $n\neq 0$ 是固定的法向量. 证明过原点的平面是 $\mathbb{R}^3$ 的二维子空间.

提示：为确定过原点的平面的维数，求出 $\mathbb{R}^3$ 的包含 n 的一个正交基.

9.53 如果 k 是特征不为 2 的域，证明对元素在 k 中的每个 $n\times n$ 矩阵 A，存在唯一的对称矩阵 B 和唯一的反称矩阵 C（即 $C^t=-C$），使得 $A=B+C$.

9.54 设 (V,f) 是内积空间，其中 V 是特征不为 2 的域 k 上的向量空间. 证明：如果 f 既是对称的又是交错的，则 $f=0$.

9.55 如果 (V,f) 是内积空间，定义 $u\perp v$ 为 $f(u,v)=0$. 证明 $\perp$ 是对称关系当且仅当 f 或者是对称的，或者是交错的.

9.56 设 (V,f) 是 f 非退化的内积空间. 如果 W 是真子空间和 $V=W\oplus W^\perp$，证明 $f\mid(W^\perp\times W^\perp)$ 是非退化的.

9.57 (i) 设 (V,f) 是内积空间，其中 V 是特征不为 2 的域 k 上的向量空间. 证明：如果 f 是对称的，则存在 V 的基 $e_1,\cdots,e_n$ 和标量 $c_1,\cdots,c_n$ 使得 $f(x,y)=\sum_i c_ix_iy_i$，其中 $x=\sum x_ie_i$ 和 $y=\sum y_ie_i$. 此外，如果 f 非退化和 k 有平方根，则可以选取基 $e_1,\cdots,e_n$ 使得 $f(x,y)=\sum_i x_iy_i$.

(ii) 如果 k 是特征不为 2 的域，则元素在 k 中的每个对称矩阵 A 和一个对角矩阵相合. 此外，如果 A 非奇异和 k 有平方根，则有某个非奇异矩阵 P 使得 $A=P^tP$. 713

9.58 举出两个 $m\times m$ 实对称矩阵的例子，它们有相同的秩和相同的判别式但不相合.

9.59 证明：对每个域 k，$\mathrm{Sp}(2,k)=\mathrm{SL}(2,k)$.

提示：根据系 9.80(ii)，我们知道如果 $P\in\mathrm{Sp}(2m,k)$，则 $\det(P)=\pm1$. 然而，命题 9.89 证明对 $P\in\mathrm{Sp}(2,k)$，$\det(P)=1$［对一切 $m\geqslant1$，$\mathrm{Sp}(2m,k)\leqslant\mathrm{SL}(2m,k)$ 成立］.

9.60 如果 A 是 $m\times m$ 矩阵满足 $A'A=I$，证明 $\begin{bmatrix} A & 0 \\ 0 & A \end{bmatrix}$ 是对称矩阵. 由此推出，如果 k 是有奇数特征的有限域，则 $O(m,k)\leqslant \mathrm{Sp}(2m,k)$.

9.61 设 (V,f) 是 f 非退化的交错空间. 证明 $T\in \mathrm{GL}(V)$ 是等距同构 [即 $T\in \mathrm{Sp}(V,f)$] 当且仅当只要 $E=x_1,y_1,\cdots,x_m,y_m$ 是 V 的辛基，则 $T(E)=Tx_1,Ty_1,\cdots,Tx_m,Ty_m$ 也是 V 的辛基.

9.6 分次代数

我们现在用多个模的张量积来构造一些有用的环. 这个课题常叫做多重线性代数.

本节中，R 始终表示交换环.

定义 如果 R-代数 A 中存在 R-子模 A^p，$p\geqslant 0$，满足

(i) $A=\sum_{p\geqslant 0}A^p$；

(ii) 对一切 $p,q\geqslant 0$，如果 $x\in A^p$ 和 $y\in A^q$，则 $xy\in A^{p+q}$；即

$$A^pA^q\subseteq A^{p+q}.$$

则 R-代数 A 称为**分次 R-代数**. 元素 $x\in A^p$ 称为 **p 次齐次的**.

注意 0 是任意次齐次的，但一个分次环中的大多数元素不是齐次的，因此没有次数. 还要注意齐次元素的任意积也是齐次的.

例 9.94 (i) 如果在多项式环 $A=R[x]$ 中定义

$$A^p=\{rx^p : r\in R\}.$$

则 $A=R[x]$ 是一个分次 R-代数. 齐次元素是单项式，和常规用法相比较，这里只有单项式（包括 0）有次数. 另一方面，在术语次数的两种用法下 x^p 都有次数 p.

(ii) 如果在多项式环 $A=R[x_1,\cdots,x_n]$ 上定义

$$A^p=\{rx_1^{e_1}x_2^{e_2}\cdots x_n^{e_n} : r\in R \text{ 和 } \sum e_i=p\};$$

714 即 A^p 由全次数为 p 的一切单项式组成，则 A 是一个分次 R-代数.

(iii) 在代数拓扑中，给空间 X 指定一个（阿贝尔的）上同调群 $H^p(X,R)$ 的序列，其中 R 是交换环和 $p\geqslant 0$，并在 $\sum_{p\geqslant 0}H^p(X,R)$ 上定义一个叫做上积的乘法，从而使其成为一个分次 R-代数. ■

正如多项式的次数十分有用一样，在分次代数中齐次元素的次数也十分有用.

定义 如果 A 和 B 都是分次 R-代数，则一个**分次映射**[⊖] 是指一个 R-映射 $f: A\to B$ 对一切 $p\geqslant 0$ 满足 $f(A^p)\subseteq B^p$.

易知一切分次 R-代数和一切分次映射形成范畴，记为 $\mathbf{Gr}_R\mathbf{Alg}$.

定义 如果 A 是分次 R-代数，则一个**分次理想**（或**齐次理想**）是指 A 中的一个双边理想 I 满足 $I=\sum_{p\geqslant 0}I^p$，其中 $I^p=I\cap A^p$.

对照第 6 章中曾经考虑过的仿射簇，在代数几何中投射簇的研究十分热烈. 这种用代数方法研究几何对象的课题涉及分次代数中的齐次理想.

⊖ 分次映射 $F: A\to B$ 有更一般的定义. 给定 $d\in\mathbb{Z}$，如果一个 k-代数映射 f 对一切 $p\geqslant 0$ 满足 $f(A^p)\subseteq B^{p+d}$，则称 f 是一个 **d 次分次映射**.

命题 9.95 设 A 和 B 都是分次 R-代数.

(i) 如果 $f: A\to B$ 是分次映射，则 $\ker f$ 是分次理想.

(ii) 如果 I 是 A 中的分次理想，并定义

$$(A/I)^p = (A^p + I)/I.$$

则 A/I 是分次 R-代数，此外，

$$A/I = \sum_p (A/I)^p \cong \sum_p A^p/(I \cap A^p) = \sum_p (A^p/I^p).$$

(iii) A 中的双边理想 I 是分次理想当且仅当 I 由齐次元素生成.

(iv) A 中的幺元 1 是次数为 0 的齐次元素.

证明 (i) 和 (ii) 的证明留作习题(十分简单).

(iii) 如果 I 是分次的，则 $I=\sum_p I^p$，从而 I 由 $\bigcup_p I^p$ 生成. 但 $\bigcup_p I^p$ 由齐次元素组成，这是因为对一切 p, $I^p = I\cap A^p \subseteq A^p$.

反之，假设 I 由齐次元素的一个集合 X 生成. 我们需要证明 $I=\sum_p (I\cap A_p)$，而这只要证明 $I\subseteq \sum_p (I\cap A_p)$，因为反包含总是成立的. 因 I 是由 X 生成的双边理想，一个典型元素 $u\in I$ 有 $u=\sum_i a_i x_i b_i$ 的形式，其中 a_i，$b_i\in A$ 和 $x_i \in X$. 现在 $u=\sum_p u_p$，其中 $u_p\in A^p$，因此只要证明每个 u_p 都在 I 中. 其实只要对一个单项 $a_i x_i b_i$ 证明就够了，所以我们略去下标 i. 因 $a=\sum a_j$ 和 $b=\sum b_\ell$，其中 a_j 和 b_ℓ 都是齐次的，我们有 $u=\sum_{j,\ell} a_j x b_\ell$；但这个和中的每个项都是齐次的，它是齐次元素 a_j，x 和 b_ℓ 的积. 于是 u_p 是那些有次数 p 的 $a_j x b_\ell$ 的和，从而 $u_p\in I$. 715

(iv) 记 $1=e_0+e_1+\cdots+e_t$，其中 $e_i\in A^i$. 如果 $a_p\in A^p$，则

$$a_p - e_0 a_p = e_1 a_p + \cdots + e_t a_p \in A^p \cap (A^{p+1}\oplus\cdots\oplus A^{p+t}) = \{0\}.$$

由此对一切齐次元素 a_p 有 $a_p=e_0 a_p$，从而对一切 $a\in A$ 有 $a=e_0 a$. 考察 $a_p=a_p 1$ (替代 $a_p=1a_p$)，类似的论证可证明对一切 $a\in A$ 有 $a=ae_0$. 所以，根据环中幺元的唯一性，$1=e_0$. ■

例 9.96 商 $R[x]/(x^{13})$ 是一个分次 R-代数. 然而，在代数 $R[x]/(x^{13}+1)$ 上没有明显的分次. 毕竟，对和 -1 的陪集一样的 x^{13} 的陪集应该指定什么次数？ ■

我们现在考虑张量积的广义结合性.

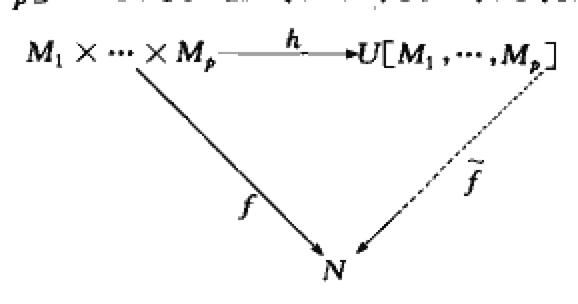
定义 设 R 是交换环，并设 $M_1,\cdots,M_p$ 是 R-模. 一个 R-**多重线性函数** $f: M_1\times\cdots\times M_p\to N$ (其中 N 是 R-模) 是指 p 个变量中的每一个都是加性的 (固定其他 $p-1$ 个变量) 函数，且如果 $1\leqslant i\leqslant p$，则

$$f(m_1,\cdots,rm_i,\cdots,m_p) = rf(m_1,\cdots,m_i,\cdots,m_p),$$

其中 $r\in R$ 且对一切 ℓ, $m_\ell\in M_\ell$.

命题 9.97 设 R 是交换环，并设 $M_1,\cdots,M_p$ 是 R-模.

(i) 存在 R-模 $U[M_1,\cdots,M_p]$，它是多重线性性提出的泛映射问题的解：



存在 R-多重线性函数 h 使得如果 f 是 R-多重线性函数，则存在唯一的 R-同态$\tilde{f}$使得图交换.

（ⅱ）如果 $f_i: M_i \to M_i'$是 R-映射，则存在唯一的 R-映射

$$u[f_1, \cdots, f_p]: U[M_1, \cdots, M_p] \to U[M_1', \cdots, M_p']$$

把 $h(m_1, \cdots, m_p) \mapsto h'(f_1(m_1), \cdots, f_p(m_p))$，其中 $h': M_1' \times \cdots \times M_p' \to U[M_1', \cdots, M_p']$.

716

证明 （ⅰ）这是定理8.74的直接推广，可用多重线性函数替代双线性函数以证明张量积的存在性. 设 F 是以 $M_1 \times \cdots \times M_p$ 为基的自由 R-模，并设 S 是 F 的子模，它由下列两种类型的元素生成：

$$(m_1, \cdots, m_i + m_i', \cdots, m_p) - (m_1, \cdots, m_i, \cdots, m_p) - (m_1, \cdots, m_i', \cdots, m_p);$$
$$(m_1, \cdots, rm_i, \cdots, m_p) - r(m_1, \cdots, m_i, \cdots, m_p),$$

其中 $m_i, m_i' \in M_i, r \in R$ 和 $1 \leqslant i \leqslant p$.

定义 $U[M_1, \cdots, M_p] = F/S$，并定义 $h: M_1 \times \cdots \times M_p \to U[M_1, \cdots, M_p]$ 为

$$h: (m_1, \cdots, m_p) \mapsto (m_1, \cdots, m_p) + S.$$

读者应验证 h 是 R-多重线性的. 证明的剩下部分只是命题8.74证明的修改，也留给读者.

（ⅱ）易知由

$$(m_1, \cdots, m_p) \mapsto h'(f_1(m_1), \cdots, f_n(m_p))$$

给出的函数 $M_1 \times \cdots \times M_p \to U[M_1', \cdots, M_p']$是 R-多重线性的，因此存在陈述中所描述的唯一的 R-同态. ■

注意生成元 $h(m_1, \cdots, m_p)$ 中不必加括号；即 $h(m_1, \cdots, m_p)$ 只依赖于 p 元组 $(m_1, \cdots, m_p)$，而不依赖于它的坐标的任何结合. 下一命题把这个构造和迭代张量积联系起来，一旦建立起这种联系，我们将改变记号 $U[M_1, \cdots, M_p]$.

命题 9.98（广义结合性） 设 R 是交换环，并设 M_1，…，M_p 是 R-模. 如果 $M_1 \otimes_R \cdots \otimes_R M_p$ 是在某种结合下的迭代张量积，则存在 R-同构 $U[M_1, \cdots, M_p] \to M_1 \otimes_R \cdots \otimes_R M_p$ 把 $h(m_1, \cdots, m_p) \mapsto m_1 \otimes \cdots \otimes m_p$.

注 我们尝试引用定理2.20：三个因子的结合性蕴涵多个因子的结合性，因为已经在命题8.84中证明了三个因子的结合律. 然而，并没有证明等式 $A \otimes_R (B \otimes_R C) = (A \otimes_R B) \otimes_R C$，而只是构造了一个同构. 有一个属于 Mac Lane 和 Stasheff 的独立的额外条件：如果不计同构结合律成立且某个“五边形”图交换，则不计同构广义结合律成立（见 Mac Lane 所著的《Categories for the Working Mathematician》，157～161页）.

证明 对 $p \geqslant 2$ 用归纳法证明. 基础步为真，因为 $U[M_1, M_2] = M_1 \otimes_R M_2$. 关于归纳步，假定

717

$$M_1 \otimes_R \cdots \otimes_R M_p = U[M_1, \cdots, M_i] \otimes_R U[M_{i+1}, \cdots, M_p].$$

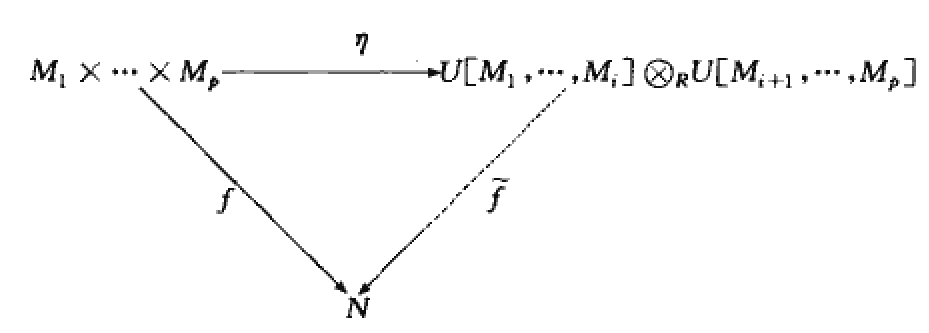
最后两个因子的结合状况已经指定；例如，

$$((M_1 \otimes_R M_2) \otimes_R M_3) \otimes_R (M_4 \otimes_R M_5) = U[M_1, M_2, M_3] \otimes_R U[M_4, M_5].$$

根据归纳假设，存在多重线性函数 $h': M_1 \times \cdots \times M_i \to M_1 \otimes_R \cdots \otimes_R M_i$ 和 $h'': M_{i+1} \times \cdots \times M_p \to M_{i+1} \otimes_R \cdots \otimes_R M_p$ 使得 $h'(m_1, \cdots, m_i) = m_1 \otimes \cdots \otimes m_i$（其结合状况和 $M_1 \otimes_R \cdots \otimes_R M_i$ 中一样）及 $h''(m_{i+1}, \cdots, m_p) = m_{i+1} \otimes \cdots \otimes m_p$（其结合状况和 $M_{i+1} \otimes_R \cdots \otimes_R M_p$ 中一样）. 归纳假设给出同构 $\varphi': U[M_1, \cdots, M_i] \to M_1 \otimes_R \cdots \otimes_R M_i$ 和 $\varphi'': U[M_{i+1}, \cdots, M_p] \to M_{i+1} \otimes_R \cdots \otimes_R M_p$ 使得 $\varphi' h' =$

$h|(M_1\times\cdots\times M_i)$ 和 $\varphi''h''=h\mid(M_{i+1}\times\cdots\times M_p)$. 根据系 8.78, $\varphi'\otimes\varphi''$ 是同构 $U[M_1,\cdots,M_i]\otimes_R U[M_{i+1},\cdots,M_p]\to M_1\otimes_R\cdots\otimes_R M_p$.

我们现在证明 $U[M_1,\cdots,M_i]\otimes_R U[M_{i+1},\cdots,M_p]$ 是关于多重线性函数的泛映射问题的解. 考虑图



其中 $\eta(m_1,\cdots,m_p)=h'(m_1,\cdots,m_i)\otimes h''(m_{i+1},\cdots,m_p)$, N 是 R-模, f 是多重线性函数. 我们需要求出同态 $\tilde f$ 使得图交换.

如果 $(m_1,\cdots,m_i)\in M_1\times\cdots\times M_i$, 由 $(m_{i+1},\cdots,m_p)\mapsto f(m_1,\cdots,m_i,h''(m_{i+1},\cdots,m_p))$ 定义的函数 $f_{(m_1,\cdots,m_i)}: M_{i+1}\times\cdots\times M_p\to N$ 是多重线性函数, 因此存在唯一的同态 $\tilde f_{(m_1,\cdots,m_i)}: U[M_{i+1},\cdots,M_p]\to N$ 使得

$$\tilde f_{(m_1,\cdots,m_i)}: h''(m_{i+1},\cdots,m_p)\mapsto f(m_1,\cdots,m_p).$$

如果 $r\in R$ 和 $1\leqslant j\leqslant i$, 则

$$\begin{aligned}\tilde f_{(m_1,\cdots,rm_j,\cdots,m_i)}(h''(m_{i+1},\cdots,m_p)) &= f(m_1,\cdots,rm_j,\cdots,m_p)\\ &= rf(m_1,\cdots,m_j,\cdots,m_i)\\ &= r\tilde f_{(m_1,\cdots,m_i)}(h''(m_{i+1},\cdots,m_p)).\end{aligned}$$

类似地, 如果 m_j, $m_j'\in M_j$, 其中 $1\leqslant j\leqslant i$, 则

$$\tilde f_{(m_1,\cdots,m_j+m_j',\cdots,m_i)}=\tilde f_{(m_1,\cdots,m_j,\cdots,m_i)}+\tilde f_{(m_1,\cdots,m_j',\cdots,m_i)}.$$

定义 $i+1$ 元函数 $M_1\times\cdots\times M_i\times U[M_{i+1},\cdots,M_p]\to N$ 为 $(m_1,\cdots,m_i,u'')\mapsto\tilde f_{(m_1,\cdots,m_i)}(u'')$, 该函数是多重线性的, 因此它给出双线性函数 $U[M_1,\cdots,M_i]\times U[M_{i+1},\cdots,M_p]\to N$, 就是 $(u',u'')\mapsto(h'(u'),h''(u''))$. 于是, 存在唯一的同态 $\tilde f: U[M_1,\cdots,M_i]\otimes_R U[M_{i+1},\cdots,M_p]\to N$ 把 $h'(m_1,\cdots,m_i)\otimes h''(m_{i+1},\cdots,m_p)\mapsto\tilde f_{(m_1,\cdots,m_i)}(h''(m_{i+1},\cdots,m_p))=f(m_1,\cdots,m_p)$; 即 $\tilde f\eta=f$. 所以, $U[M_1,\cdots,M_i]\otimes_R U[M_{i+1},\cdots,M_p]$ 是泛映射问题的解. 由这种解的唯一性, 存在同构 $\theta: U[M_1,\cdots,M_p]\to U[M_1,\cdots,M_i]\otimes_R U[M_{i+1},\cdots,M_p]$ 使得 $\theta h(m_1,\cdots,m_p)=h'(m_1,\cdots,m_i)\otimes h''(m_{i+1},\cdots,m_p)=\eta(m_1,\cdots,m_p)$. 最后, $(\varphi'\otimes\varphi'')\theta$ 是所要的同构 $U[M_1,\cdots,M_p]\cong M_1\otimes_R\cdots\otimes_R M_p$. ■ [718]

我们现在放弃命题 9.97 中的记号; 从现在开始, 记

$$\begin{aligned}U[M_1,\cdots,M_p] &= M_1\otimes_R\cdots\otimes_R M_p,\\ h(m_1,\cdots,m_p) &= m_1\otimes\cdots\otimes m_p,\\ u[f_1,\cdots,f_p] &= f_1\otimes\cdots\otimes f_p.\end{aligned}$$

命题 9.99 如果 R 是交换环且 A 和 B 是 R-代数, 如果定义 $(a\otimes b)(a'\otimes b')=aa'\otimes bb'$, 则张量积 $A\otimes_R B$ 是 R-代数.

证明 首先, 根据系 8.81, $A\otimes_R B$ 是 R-模. 设 $\mu: A\times A\to A$ 和 $\nu: B\times B\to B$ 分别是代数 A 和 B 上给定的乘法. 我们需要证明 $A\otimes_R B$ 上存在命题陈述的乘法; 即存在 R-双线性函数

$\lambda:(A\otimes_R B)\times(A\otimes_R B)\to A\otimes_R B$，其中 $\lambda:(a\otimes b,a'\otimes b')\mapsto aa'\otimes bb'$．这样的函数 λ 是存在的，因为它是复合

$$\begin{aligned}(A\otimes_R B)\times(A\otimes_R B)&\to(A\otimes_R B)\otimes(A\otimes_R B)\\&\to(A\otimes_R A)\times(B\otimes_R B)\\&\to A\otimes_R B.\end{aligned}$$

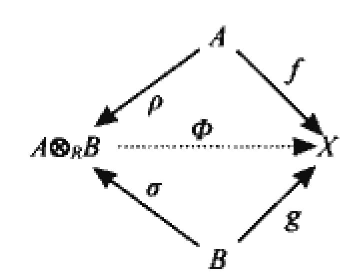
第一个函数是 $(a\otimes b,\ a'\otimes b')\mapsto a\otimes b\otimes a'\otimes b'$（它是命题 8.82 中的双线性函数）；第二个是 $1\otimes\tau\otimes 1$，其中 $\tau:B\otimes_R A\to A\otimes_R B$ 把 $b\otimes a\mapsto a\otimes b$（根据命题 8.83 和命题 9.98，存在这个函数）；第三个是 $\mu\otimes\nu$. 现在容易验证 R-模 $A\otimes_R B$ 是 R-代数. ■

例 9.100 在习题 8.48 中，我们看到存在阿贝尔群的同构：$\mathbb{I}_m\otimes\mathbb{I}_n\cong\mathbb{I}_d$，其中 $d=(m,n)$. 由此，如果$(m,n)=1$，则$\mathbb{I}_m\otimes\mathbb{I}_n\cong\{0\}$. 当然，如果把$\mathbb{I}_m$ 和$\mathbb{I}_n$ 看作$\mathbb{Z}$-代数，这个张量积仍然是 $\{0\}$. 于是，在这种情形下，张量积是零环. 如果在环的定义中坚持 $1\neq 0$，则环的张量积将不是恒有定义的. ■

我们现在证明代数的张量积是一个“诚实的”构造.

命题 9.101 *如果 R 是交换环且 A 和 B 是交换 R-代数，则 $A\otimes_R B$ 是交换 R-代数的范畴中的余积.*

证明 定义 $\rho:A\to A\otimes_R B$ 为 $\rho:a\mapsto a\otimes 1$，并定义 $\sigma:B\to A\otimes_R B$ 为 $\sigma:b\mapsto 1\otimes b$. 设 X 是交换 R-代数，并考虑图



719

其中 f 和 g 是R-代数映射. 易知由 $(a,b)\mapsto f(a)g(b)$ 给出的函数 $\varphi:A\times B\to X$ 是R-双线性的，因此存在唯一的 R-模的映射 $\Phi:A\otimes_R B\to X$ 满足 $\Phi(a\otimes b)=f(a)g(b)$．剩下要证明 Φ 是R-代数映射，为此只要证明 $\Phi((a\otimes b)(a'\otimes b'))=\Phi(a\otimes b)\Phi(a'\otimes b')$．现在

$$\begin{aligned}\Phi((a\otimes b)(a'\otimes b'))&=\Phi(aa'\otimes bb')\\&=f(a)f(a')g(b)g(b').\end{aligned}$$

另一方面，$\Phi(a\otimes b)\Phi(a'\otimes b')=f(a)g(b)f(a')g(b')$．因 X 是交换的，所以 Φ 保持乘法. ■

双模可以看作一个适当的环上的左模.

系 9.102 *设 R 和 S 都是 k-代数，其中 k 是交换环. 每个(R,S)-双模 M 是一个左$R\otimes_k S^{\mathrm{op}}$-模，其中*

$$(r\otimes s)m=rms.$$

证明 由 $(r,s,m)\mapsto rms$ 给出的函数是 $R\times S^{\mathrm{op}}\times M\to M$ 是 k-三线性的，这可以用来证明 $(r\otimes s)m=rms$ 是合理定义的. 记 S^{op} 中的积为 $s*s'$；即 $s*s'=s's$．模的定义中只有公理（ⅲ）不是显而易见的：如果 $a,a'\in R\otimes_k S^{\mathrm{op}}$，则 $(aa')m=a(a'm)$，只要对 $R\otimes_k S^{\mathrm{op}}$ 的生成元 $a=r\otimes s$ 和 $a'=r'\otimes s'$ 验证就够了. 但

$$\begin{aligned}[(r\otimes s)(r'\otimes s')]m&=[rr'\otimes s*s']m\\&=(rr')m(s*s')\end{aligned}$$

$$= (rr')m(s's)$$
$$= r(r'ms')s.$$

另一方面，

$$(r \otimes s)[(r' \otimes s')m] = (r \otimes s)[r'(ms')] = r(r'ms')s. \quad ■$$

定义　如果 k 是交换环，A 是 k-代数，则它的**包络代数**是

$$A^e = A \otimes_k A^{\mathrm{op}}.$$

系 9.103　如果 k 是交换环，A 是 k-代数，则 A 是一个左 A^e-模，它的子模是双边理想．如果 A 是单 k-代数，则 A 是单 A^e-模．

证明　因 k-代数 A 是 (A,A)-双模，所以它是左 A^e-模． ■

命题 9.104　如果 k 是交换环和 A 是 k-代数，则

$$\mathrm{End} A^e(A) \cong Z(A).$$

证明　如果 $f: A \to A$ 是 A^e-映射，则它是只把 A 看作左 A-模的映射．运用命题 8.12 可知 f 由 $z = f(1)$ 确定，这是因为对一切 $a \in A, f(a) = f(a1) = af(1) = az$．另一方面，因 f 也是把 A 看作右 A-模的映射，有 $f(a) = f(1a) = f(1)a = za$．所以，$z = f(1) \in Z(A)$；即映射 $\varphi: f \mapsto f(1)$ 是映射 $\mathrm{End}_{A^e}(A) \to Z(A)$．如果 $z \in Z(A)$，则 $f(a) = za$ 是 A^e-自同态满足 $\varphi(f) = z$，所以 φ 是满射；如果 $f \in \mathrm{End}_{A^e}(A)$ 和 $f(1) = 0$，则 $f = 0$，所以 φ 是单射． ■

我们现在在 R-模 M 上构造张量代数．当 M 是以 X 为基的自由 R-模时，张量代数可以看作以 X 为基的自由 R-代数；即它是 R 上变量 X 不交换的多项式环．

定义　设 R 是交换环，并设 M 是 R-模．定义

$$T^0(M) = R,$$
$$T^1(M) = M,$$
$$T^p(M) = M \otimes_R \cdots \otimes_R M\ (p\ 次)，如果\ p \geqslant 2.$$

注　许多作者把 $T^p(M)$ 记为 $\otimes^p M$．在命题 9.97 中，$T^p(M)$ 原先记为 $U[M_1, \cdots, M_p]$（这里 $M_i = M$），后来把它改为 $M_1 \otimes \cdots \otimes M_p$，因为这个记号容易记忆．然而，我们提醒读者 $T^p(M)$ 是由符号 $m_1 \otimes \cdots \otimes m_p$ 生成的，其中不出现括号．

命题 9.105　如果 M 是 R-模，则存在分次 R-代数

$$T(M) = \sum_{p \geqslant 0} T^p(M)$$

且有 $r \in R$ 在 $T^q(M)$ 上的作用，它由

$$r(y_1 \otimes \cdots \otimes y_q) = (ry_1) \otimes y_2 \otimes \cdots \otimes y_q = (y_1 \otimes \cdots \otimes y_q)r$$

给出，并且对 $p, q \geqslant 1$ 有乘法 $T^p(M) \times T^q(M) \to T^{p+q}(M)$，它由

$$(x_1 \otimes \cdots \otimes x_p, y_1 \otimes \cdots \otimes y_q) \mapsto x_1 \otimes \cdots \otimes x_p \otimes y_1 \otimes \cdots \otimes y_q$$

给出．

证明　首先，用陈述中的公式定义两个齐次元素的积．现在乘法 $\mu: T(M) \times T(M) \to T(M)$ 必是

$$\mu: \Big(\sum_p x_p, \sum_q y_q\Big) \mapsto \sum_{p,q} x_p \otimes y_q,$$

其中 $x_p \in T^p(M)$ 和 $y_q \in T^q(M)$．因为在所描述的 $T^p(M)$ 的生成元 $m_1 \otimes \cdots \otimes m_p$ 中不需要括号，所以乘法是结合的，因为乘法是 R-双线性的，所以分配律成立．最后，$1 \in k = T^0(M)$ 是幺元，R 的

每个元素和 $T(M)$ 的每个元素可交换，以及 $T^p(M)T^q(M) \subseteq T^{p+q}(M)$，因此 $T(M)$ 是分次R-代数. ■

读者可以验证，如果 $M = R$，则 $T(M) \cong R[x]$.

定义 如果 R 是交换环和 M 是R-模，则 $T(M)$ 叫做 M 上的**张量代数**.

如果 R 是交换环且 A 和 B 是R-模，定义 A 和 B 上**长**为 $p \geqslant 0$ 的**字**为形如

$$W(A,B)_p = T^{e_1}(A) \otimes_R T^{f_1}(B) \otimes_R \cdots \otimes_R T^{e_r}(A) \otimes_R T^{f_r}(B)$$

的R-模，其中 $\sum_i (e_i + f_i) = p$，一切 e_i, f_i 都是整数，$e_1 \geqslant 0, f_r \geqslant 0$，其他指数都是正的.

命题 9.106 如果 A 和 B 都是R-模，则对一切 $p \geqslant 0$，

$$T^p(A \oplus B) \cong \sum_{j=0}^{p} W(A,B)_j \otimes_R W'(A,B)_{p-j},$$

其中 $W(A,B)_j, W'(A,B)_{p-j}$ 遍历长分别为 j 和 $p-j$ 的一切字.

证明 对 $p \geqslant 0$ 用归纳法证明. 关于基础步，

$$T^0(A \oplus B) = R \cong R \otimes_R R \cong T^0(A) \otimes_R T^0(B).$$

关于归纳步，

$$\begin{aligned} T^{p+1}(A \oplus B) &= T^p(A \oplus B) \otimes_R (A \oplus B) \\ &\cong (T^p(A \oplus B) \otimes_R A) \oplus (T^p(A \oplus B) \otimes_R B) \\ &\cong \sum_{j=0}^{p} W(A,B)_j \otimes_R W'(A,B)_{p-j} \otimes_R X, \end{aligned}$$

722 其中 $X \cong A$ 或 $X \cong B$. 由于长为 $p-j+1$ 的每个字都有 $W'(A,B) \otimes_R X$ 的形式，证明完成. ■

命题 9.107 张量代数定义了一个函子 T: ${}_R\mathbf{Mod} \to \mathbf{Gr}_R\mathbf{Alg}$. 此外，$T$ 保持满射.

证明 我们已经在每个R-模 M 上定义了 T：它就是张量代数 $T(M)$. 如果 $f: M \to N$ 是R-同态，则命题 9.97 对每个 p 提供映射

$$f \otimes \cdots \otimes f: T^p(M) \to T^p(N),$$

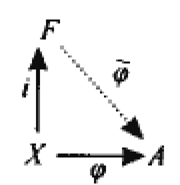
它给出R-代数映射 $T(M) \to T(N)$. 容易验证 T 保持恒等映射和复合.

假定 $f: M \to N$ 是满射R-映射. 如果 $n_1 \otimes \cdots \otimes n_p \in T^p(N)$，则对一切 i，f 的满射性提供 $m_i \in M$ 使得 $f(m_i) = n_i$，因此，

$$T(f): m_1 \otimes \cdots \otimes m_p \mapsto n_1 \otimes \cdots \otimes n_p.$$ ■

我们现在把自由模的概念推广到自由代数.

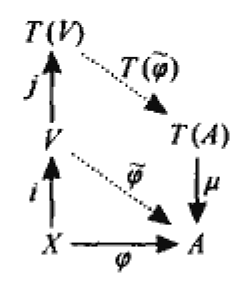
定义 如果 X 是R-代数 F 的子集，且对每个R-代数 A 和每个函数 $\varphi: X \to A$，存在唯一的R-代数映射 $\tilde{\varphi}$ 使得对一切 $x \in X$ 有 $\tilde{\varphi}(x) = \varphi(x)$，则称 F 是以 X 为基的**自由 R-代数**. 换句话说，下图交换，其中 $i: X \to F$ 是包含映射.



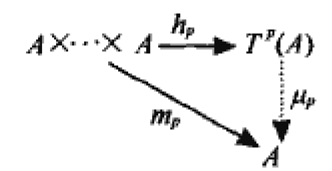
下一命题中我们把分次R-代数仅看作R-代数.

命题 9.108 如果 V 是以 X 为基的自由R-模，其中 R 是交换环，则 $T(V)$ 是以 X 为基的自由R-代数.

证明 考虑图



其中 $i: X \to V$ 和 $j: V \to T(V)$ 都是包含映射，且 A 是 R-代数．因为 V 是以 X 为基的自由 R-模，所以把 A 只看作 R-模给出 R-模映射 $\widetilde{\varphi}: V \to A$．运用函子 T 给出 R-代数映射 $T(\widetilde{\varphi}): T(V) \to T(A)$．关于 R-代数映射 $T(V) \to A$ 的存在性，只要定义一个 R-代数映射 $\mu: T(A) \to A$ 使得复合 $\mu \circ T(\widetilde{\varphi})$ 是扩张 φ 的 R-代数映射．对每个 p，考虑图 [723]



其中 $h_p: (a_1, \cdots, a_p) \mapsto a_1 \otimes \cdots \otimes a_p$ 和 $m_p: (a_1, \cdots a_p) \mapsto a_1 \cdots a_p$，后一个是元素 $a_1, \cdots, a_p$ 在 R-代数 A 中的积．当然，m_p 是 R-双线性的，因此它诱导出一个 R-映射 μ_p 使得图交换．现在定义 $\mu: T(A) \to A$ 为 $\mu = \sum_p u_p$．为证明 μ 是可乘的，只要证明

$$\mu_{p+q}((a_1 \otimes \cdots \otimes a_p) \otimes (a'_1 \otimes \cdots \otimes a'_q)) = \mu_p(a_1 \otimes \cdots \otimes a_p)\mu_q(a'_1 \otimes \cdots \otimes a'_q).$$

但这个等式来自 A 中的结合律：

$$(a_1 \cdots a_p)(a'_1 \cdots a'_q) = a_1 \cdots a_p a'_1 \cdots a'_q.$$

最后，R-代数映射的唯一性是由 V 生成作为 R-代数的 $T(V)$ 而得［毕竟，$T(V)$ 中的每个齐次元素都是 1 次元素的积］. ■

系 9.109 设 R 是交换环.

（ⅰ）如果 A 是 R-代数，则存在满射 R-代数映射 $T(A) \to A$.

（ⅱ）每个 R-代数 A 都是自由 R-代数的一个商.

证明 （ⅰ）把 A 只看作 R-模．对每个 $p \geq 2$，乘法 $A^p \to A$ 是 R-多重线性的，从而存在唯一的 R-模映射 $T^p(A) \to A$．但这些映射可以组合成一个 R-模映射 $T(A) = \sum_p T^p(A) \to A$．因为 A 有幺元 1，所以这个映射是满射且易知它是 R-代数映射；即它保持乘法.

（ⅱ）设 V 是自由 R-模，且存在满射 R-映射 $\varphi: V \to A$．根据命题 9.107，诱导映射 $T(\varphi): T(V) \to T(A)$ 是满射．现在 $T(V)$ 是自由 R-代数，如果把 $T(\varphi)$ 和满射 $T(A) \to A$ 复合，则 A 是 $T(V)$ 的商. ■

定义 如果 R 是交换环和 V 是以 X 为基的自由 R-模，则 $T(V)$ 叫做 R 上变量 X 非交换的多项式环，记为 $R\langle X\rangle$. [724]

如果 V 是以 X 为基的自由 R-模，则 $T(V)$ 中的每个元素 u 有唯一的表达式

$$u = \sum_{\substack{p \geq 0 \\ i_1, \cdots, i_p}} r_{i_1, \cdots, i_p} x_{i_1} \otimes \cdots \otimes x_{i_p},$$

其中 $r_{i_1, \cdots, i_p} \in R$ 和 $x_{i_j} \in X$．抹去张量积符号得到这种多项式的常用记号．例如，如果，$X = \{x, y\}$，则

$$u = r_0 + r_1 x + r_2 y + r_3 x^2 + r_4 y^2 + r_5 xy + r_6 yx + \cdots.$$

例 9.110 正如模那样，我们现在可以用生成元和关系构造环（Z-代数）. 左诺特的而非右诺特的环的第一个例子由迪厄多内（J. Dieudonné）给出；它是由元素 x 和 y 生成并满足关系 $yx=0$ 和 $y^2=0$ 的环 R. 环 R 的存在性现在是容易证明的：设 V 是以 u，v 为基的自由阿贝尔群，设 $R=\left(\sum_{p\geq 0} T^p(V)\right)/I$，其中 I 是由 vu 和 v^2 生成的双边理想，令 $x=u+I$ 和 $y=v+I$. 注意，因为理想 I 是由 2 次齐次元素生成的，所以有 $T^1(V)=V\cap I=\{0\}$，从而 $x\neq 0$ 和 $y\neq 0$. ■

我们现在提出一类环，它推广了交换环.

定义 如果 k 是域[⊖]，则 k-代数 A 上的**多项式恒等式**是指元素 $f(X)\in k\langle X\rangle$（$k$ 上变量 X 非交换的多项式环），它在 A 中的所有代换都是 0.

例如，如果 $f(x,y)=xy-yx\in k\langle x,y\rangle$，则 f 是在一个满足对一切 a，$b\in A$ 有 $ab-ba=0$ 的 k-代数 A（即 A 是交换的）上的多项式恒等式.

这里是精确定义. 每个函数 $\varphi: X\to A$ 扩张为 k-代数映射 $\tilde{\varphi}: k\langle X\rangle\to A$，$f(X)$ 是 A 上的多项式恒等式当且仅当对一切函数 $\varphi: X\to A$ 有 $f(X)\in\bigcap_{\varphi}\ker\tilde{\varphi}$.

定义 一个 k-代数 A 如果满足至少一个系数是 1 的恒等式，则称 A 为 **PI-代数**（满足一个多项式恒等式的代数）.

每个由 n 个元素生成的 k-代数满足**标准恒等式**

$$s_{n+1}(x_1,\cdots,x_{n+1})=\sum_{\sigma\in S_{n+1}}\operatorname{sgn}(\sigma)x_{\sigma(1)}\cdots x_{\sigma(n+1)}.$$

可以证明矩阵代数 $\mathrm{Mat}_n(k)$满足标准恒等式 s_{n^2+1}，阿米苏尔（S. A. Amitsur）和列维茨基（J. Levitzki）证明 $\mathrm{Mat}_n(k)$ 满足 s_{2n}；此外，$2n$ 是这种多项式恒等式中次数最小的. 有一个短证明属于 S. Rosset，"A New Proof of the Amitsur - Levitski Identity，" *Israel Journal of Mathematics* 23，1976，187～188 页.

725

定义 k-代数 A 上的**中心多项式恒等式**是指 A 上的一个多项式 $f(X)\in k\langle X\rangle$，它的一切值 $f(a_1,a_2,\cdots)$（a_i 遍历 A 的一切元素）都在 $Z(A)$ 中.

E. Formanek 和 Yu. P. Razmyslov 独立地证明了 $\mathrm{Mat}_n(k)$ 满足中心多项式恒等式.

有定理证明 PI-代数在几个方面和交换代数有相像的性态. 例如，回忆如果环 R 有忠实单左R-模，则 R 是本原的；如果 R 是交换的，则 R 是域卡普兰斯基证明一个 PI-代数的每个本原商是单的，且在它的中心上是有限维的. 读者可参考 Procesi 的《Rings with Polynomial Identities》.

当前研究的另一个重要领域涉及非交换代数几何. 本质上，它涉及研究 $k\langle x_1,\cdots,x_n\rangle$（替代 $k[x_1,\cdots,x_n]$）中现在定义为理想的零点的簇.

习题

9.62 （i）如果 k 是域 K 的子域，证明环 $K\otimes_k k[x]$ 和 $K[x]$ 同构.

（ii）假设 k 是域，$p(x)\in k[x]$ 是不可约的，$K=k(\alpha)$，其中 α 是 $p(x)$ 的一个根. 证明：和环一样，$K\otimes_k K\cong K[x]/(p(x))$，其中 $(p(x))$ 是 $K[x]$ 中由 $p(x)$ 生成的主理想.

（iii）多项式 $p(x)$虽然在 $k[x]$中不可约，但有可能在 $K[x]$中进行因子分解. 举出一个例子证明$K\otimes_k K$未必半单.

⊖ 当然，可以把这个定义扩张为 k 是交换环.

(iv) 证明：如果 K/k 是有限可分扩张，则 $K\otimes_k K$ 是半单的.（逆命题也成立.）

9.63 设 m 和 n 是正整数，并设 $d=\gcd(m,n)$. 证明作为交换环有 $\mathbb{I}_m\otimes_{\mathbb{Z}}\mathbb{I}_n\cong\mathbb{I}_d$.

提示：见习题 8.48.

9.64 如果 $A\cong A'$ 和 $B\cong B'$ 都是 k-代数，其中 k 是交换环，证明作为 k-代数有 $A\otimes_k B\cong A'\otimes_k B'$.

9.65 如果 k 是交换环且 A，B 是 k-代数，证明

$$(A\otimes_k B)^{op}\cong A^{op}\otimes_k B^{op}.$$

9.66 如果 R 是交换 k-代数，其中 k 是域，且如果 G 是群，证明 $R\otimes_k kG\cong RG$.

9.67 (i) 如果 k 是交换环 R 的子环，证明作为 R-代数有 $R\otimes_k k[x]\cong R[x]$.

(ii) 如果 $f(x)\in k[x]$ 和 (f) 是由 $f(x)$ 生成的 $k[x]$ 中的主理想，证明 $R\otimes_k(f)$ 是由 $f(x)$ 生成的 $R[x]$ 中的主理想. 更精确地说，存在交换图

$$\begin{array}{ccccc} 0\longrightarrow & E\otimes_k(f) & \longrightarrow & E\otimes_k k[x] \\ & \downarrow & & \downarrow \\ 0\longrightarrow & (f)_E & \longrightarrow & E[x] \end{array}$$

726

(iii) 设 k 是域和 $E\cong k[x]/(f)$，其中 $f(x)\in k[x]$ 是不可约的. 证明 $E\otimes_k E\cong E[x]/(f)_E$，其中 $(f)_E$ 是由 $f(x)$ 生成的 $E[x]$ 中的主理想.

(iv) 举出一个域扩张 E/k 的例子使得 $E\otimes_k E$ 不是域.

提示：如果 $f(x)\in k[x]$ 在 $E[x]$ 中因子分解为 $g(x)h(x)$，其中 $(g,h)=1$，则可用孙子剩余定理.

9.68 设 k 是域并设 $f(x)\in k[x]$ 是不可约的. 如果 K/k 是域扩张，则 $f(x)=p_1(x)^{e_1}\cdots p_n(x)^{e_n}\in K[x]$，其中 $p_i(x)$ 是 $K[x]$ 中不同的不可约多项式和 $e_i\geqslant 1$.

(i) 证明 $f(x)$ 是可分的当且仅当一切 $e_i=1$.

(ii) 证明有限域扩张 K/k 是可分的当且仅当 $K\otimes_k K$ 是半单环.

提示：首先考察 K/k 是单扩张，从而存在正合列 $0\to(f)\to k[x]\to K\to 0$. 其次，用孙子剩余定理.

9.69 证明例 9.110 中的环 R 是左诺特的但不是右诺特的.

提示：见嘉当（Cartan）和艾伦伯格（Eilenberg）的《Homological Algebra》, 16 页.

9.70 如果 G 是群，则 k-代数 A 称为 G-**分次代数**如果对一切 $g\in G$，存在 k-子模 A^g 满足

(i) $A=\sum_{g\in G}A^g$.

(ii) 对一切 $g,h\in G, A^gA^h\subseteq A^{gh}$.

一个 $\mathbb{I}_2$-分次代数称为**超代数**. 如果 A 是 G-分次代数和 e 是 G 的幺元，证明 $1\in A^e$.

9.71 如果 A 是由 n 个元素生成的 k-代数，证明 A 满足 725 页的标准恒等式.

9.7 可除代数

代数的张量积还是代数，这一事实用于除环的研究.

定义 域 k 上的**可除代数**是指把除环看作它的中心 k 上的代数.

我们先考虑更广的单代数类.

定义 如果域 k 上的一个 k-代数 A 是有限维的[⊖]、单的（没有 A 和 $\{0\}$ 之外的其他双边理想）且它的中心 $Z(A)=k$，则称 A 为**中心单代数**.

⊖ 有些作者没有有限维的假设.

记号 如果 A 是域 k 上的代数，则记

727

$$[A:k]=\dim_k(A).$$

例 9.111 （ⅰ）在中心 k 上是有限维的每个可除代数 Δ 都是中心单 k-代数. 四元数 $\mathbb{H}$ 是中心单 $\mathbb{R}$-代数，每个域是它自身上的中心单代数. 希尔伯特给出一个无限维可除代数的例子（见 Drozd-Kirichenko 所著的《Finite Dimensional Algebras》，81 页）.

（ⅱ）如果 k 是域，则 $\mathrm{Mat}_n(k)$ 是中心单 k-代数.

（ⅲ）如果 A 是中心单 k-代数，则它的对立代数 A^{op} 也是中心单 k-代数. ■

定理 9.112 设 A 是中心单 k-代数. 如果 B 是单 k-代数，则 $A\otimes_k B$ 是中心单 $Z(B)$-代数. 特别地，如果 B 是中心单 k-代数，则 $A\otimes_k B$ 是中心单 k-代数.

证明 每个 $x\in A\otimes_k B$ 有形如

$$x=a_1\otimes b_1+\cdots+a_n\otimes b_n \tag{1}$$

的表达式，其中 $a_i\in A$ 和 $b_i\in B$. 对非零 x，如果没有少于 n 项的表达式，则定义 x 的长度为 n. 我们断言如果 x 的长度为 n，即等式 (1) 是最短的这种表达式，则 $b_1,\cdots,b_n$ 是 B 中的线性无关表（看作 k 上的向量空间）. 否则，存在某个 j 和不全为零的 $u_i\in k$ 使得

$b_j=\sum_i u_i b_i$. 代入且合并同类项得

$$x=\sum_{i\neq j}(a_i+u_i a_j)\otimes b_i,$$

它是 x 的更短的表达式.

设 $I\neq\{0\}$ 是 $A\otimes_k B$ 中的双边理想. 选取 x 为 I 中长度最小的（非零）元素，并假定等式 (1) 是 x 的最短表达式. 现在 $a_1\neq 0$. 因 Aa_1A 是 A 中的双边理想，单性给出 $A=Aa_1A$. 因此，存在 A 中的元素 a_p' 和 a_p'' 使得 $1=\sum_p a_p' a_1 a_p''$. 因 I 是双边理想，

$$x'=\sum_p a_p' x a_p''=1\otimes b_1+c_2\otimes b_2+\cdots+c_n\otimes b_n \tag{2}$$

在 I 中，其中对 $i\geqslant 2$ 有 $c_i=\sum_p a_p' a_i a_p''$. 现阶段我们还不知道是否 $x'\neq 0$，但我们知道对每个 $a\in A,(a\otimes 1)x'-x'(a\otimes 1)\in I$. 现在

$$(a\otimes 1)x'-x'(a\otimes 1)=\sum_{i\geqslant 2}(ac_i-c_ia)\otimes b_i. \tag{3}$$

首先，这个元素是 0，否则它是 I 中长度比 x 小的元素. 因 b_1，…，b_n 是线性无关表，它生成的 k-子空间是 $\langle b_1,\cdots,b_n\rangle=\langle b_1\rangle\oplus\cdots\oplus\langle b_n\rangle$，从而

728

$$A\otimes_k\langle b_1,\cdots,b_n\rangle=A\otimes_k\langle b_1\rangle\oplus\cdots\oplus A\otimes_k\langle b_n\rangle.$$

由此等式(3)中的每一项 $(ac_i-c_ia)\otimes b_i$ 必都是 0. 因此对一切 $a\in A,ac_i=c_ia$；即每个 $c_i\in Z(A)=k$. 等式(2)变成

$$\begin{aligned}x'&=1\otimes b_1+c_2\otimes b_2+\cdots+c_n\otimes b_n\\&=1\otimes b_1+1\otimes c_2b_2+\cdots+1\otimes c_nb_n\\&=1\otimes(b_1+c_2b_2+\cdots+c_nb_n).\end{aligned}$$

现在因为 $b_1,\cdots,b_n$ 是线性无关表，$b_1+c_2b_2+\cdots+c_nb_n\neq 0$，从而 $x'\neq 0$. 所以 I 包含形如 $1\otimes b$ 的非零元素. 但 B 的单性给出 $BbB=B$，从而存在 $b_q',b_q''\in B$ 使得 $\sum_q b_q' b b_q''=1$. 因此，I 包含 $\sum_q(1\otimes b_q')(1\otimes b)(1\otimes b_q'')=1\otimes 1$，它是 $A\otimes_k B$ 中的单位. 所以 $I=A\otimes_k B$ 和 $A\otimes_k B$ 是单的.

我们现在寻找 $A\otimes_k B$ 的中心. 显然, $k\otimes_k Z(B)\subseteq Z(A\otimes_k B)$. 关于反包含, 设 $z\in Z(A\otimes_k B)$ 是非零元素, 并设

$$z = a_1\otimes b_1+\cdots+a_n\otimes b_n$$

是 z 的最短的这种表达式. 和前面的论证一样, b_1, …, b_n 是 k 上的线性无关表. 对每个 $a\in A$, 有

$$0=(a\otimes 1)z-z(a\otimes 1)=\sum_i(aa_i-a_ia)\otimes b_i.$$

由此和前面一样, 对每个 i, $(aa_i-a_ia)\otimes b_i=0$. 因此 $aa_i-a_ia=0$, 从而对一切 $a\in A$, $aa_i=a_ia$ 和每个 $a_i\in Z(A)=k$. 于是, $z=1\otimes x$, 其中 $x=a_1b_1+\cdots+a_nb_n\in B$. 但如果 $b\in B$, 则

$$0=z(1\otimes b)-(1\otimes b)z=(1\otimes x)(1\otimes b)-(1\otimes b)(1\otimes x)=1\otimes(xb-bx).$$

所以, $xb-bx=0$ 和 $x\in Z(B)$. 由此正如所要的那样, $z\in k\otimes_k Z(B)$. ■

一般来说, 单 k-代数的张量积未必是单的; 我们必须注意到中心. 在习题9.67(iv)中我们看到, 如果 E/k 是域扩张, 则 $E\otimes_k E$ 未必是域. 在下一例中将会看到, 可除代数的张量积未必是可除代数.

例 9.113 代数$\mathbb{C}\otimes_{\mathbb{R}}\mathbb{H}$ 是 8 维$\mathbb{R}$-代数, 但它也是 4 维$\mathbb{C}$-代数: 一个基是

$$1=1\otimes 1, 1\otimes i, 1\otimes j, 1\otimes k.$$

729

我们让读者证明有

$$1\otimes 1\mapsto\begin{bmatrix}1&0\\0&1\end{bmatrix},$$

$$1\otimes i\mapsto\begin{bmatrix}i&0\\0&-i\end{bmatrix},$$

$$1\otimes j\mapsto\begin{bmatrix}0&1\\-1&0\end{bmatrix},$$

$$1\otimes k\mapsto\begin{bmatrix}0&i\\i&0\end{bmatrix}$$

的向量空间同构 $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{H}\to\mathrm{Mat}_2(\mathbb{C})$ 是$\mathbb{C}$-代数同构. ■

另一种证明 $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{H}\cong\mathrm{Mat}_2(\mathbb{C})$ 的方法来自例 8.71(ii). 注意

$$\mathbb{R}\mathbf{Q}\cong\mathbb{R}\times\mathbb{R}\times\mathbb{R}\times\mathbb{R}\times\mathbb{H};$$

用$\mathbb{C}$作张量积得

$$\mathbb{C}\mathbf{Q}\cong\mathbb{C}\otimes_{\mathbb{R}}\mathbb{R}\mathbf{Q}\cong\mathbb{C}\times\mathbb{C}\times\mathbb{C}\times\mathbb{C}\times\mathbb{C}\otimes_{\mathbb{R}}\mathbb{H}.$$

由韦德伯恩定理中的唯一性得 $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{H}\cong\mathrm{Mat}_2(\mathbb{C})$.

下一定理把例 9.113 中的同构的存在性放到中心单代数中.

定理 9.114 *设 k 是域并设 A 是中心单 k-代数.*

(i) 如果 $\overline{k}$ 是 k 的代数闭包, 则存在整数 n 使得

$$\overline{k}\otimes_k A\cong\mathrm{Mat}_n(\overline{k}).$$

(ii) 如果 A 是中心单 k-代数, 则存在整数 n 使得

$$[A:k]=n^2.$$

证明 (i) 根据定理 9.112, $\overline{k}\otimes_k A$ 是单$\overline{k}$-代数. 因此, 韦德伯恩定理 (其实是系 8.63) 对某个 $n\geq 1$ 和某个除环 D 给出 $\overline{k}\otimes_k A\cong\mathrm{Mat}_n(D)$. 因 D 是 $\overline{k}$ 上有限维可除代数, Molien 的系 8.65 中的论证证明 $D=\overline{k}$.

（ⅱ）我们断言 $[A:k]=[\bar{k}\otimes_k A:\bar{k}]$，这是因为如果 $a_1,\cdots,a_m$ 是 A 在 k 上的基，则 $1\otimes a_1,\cdots,1\otimes a_m$ 是 $\bar{k}\otimes_k A$ 在 $\bar{k}$ 上的基（实质上是因为张量积与直和可交换）．所以

$$[A:k]=[\bar{k}\otimes_k A:\bar{k}]=[\mathrm{Mat}_n(\bar{k}):\bar{k}]=n^2. \qquad \blacksquare$$

四元数 $\mathbb{H}$ 的除环是中心单 $\mathbb{R}$-代数，因此它的维数 $[\mathbb{H}:\mathbb{R}]$ 必是一个平方数（维数是 4）．此外，因 $\mathbb{C}$ 是代数闭的，定理 9.114 给出 $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{H}\cong\mathrm{Mat}_2(\mathbb{C})$（例 9.113 展示了一个明确的同构）．

730

定义 中心单 k-代数的一个**分裂域**是指域扩张 E/k，对此存在整数 n 使得 $E\otimes_k A\cong\mathrm{Mat}_n(E)$．

定理 9.114 说域 k 的代数闭包 $\bar{k}$ 对每个中心单 k-代数 A 是一个分裂域．我们要证明恒存在一个分裂域是 k 的有限扩张，为此先建立几个工具．

定义 如果 A 是 k-代数和 $X\subseteq A$ 是子集，则它的**中心化子** $C_A(X)$ 定义为

$$C_A(X)=\{a\in A: \text{对每个 } x\in X \text{ 有 } ax=xa\}.$$

容易验证中心化子恒为子代数．

下一个证明的关键思想是 A 的子代数 B 使 A 成为一个 (B,A)-双模，且 B 的中心化子可以用一个自同态环来描述（这一思想在森田定理的证明中使用过）．

定理 9.115（双重中心化子） 设 A 是域 k 上的中心单代数，并设 B 是 A 的单子代数．

（ⅰ）$C_A(B)$ 是单 k-代数．

（ⅱ）对某个可除代数 Δ 有 $B\otimes_k A^{\mathrm{op}}\cong\mathrm{Mat}_s(\Delta)$ 和 $C_A(B)\cong\mathrm{Mat}_r(\Delta^{\mathrm{op}})$，其中 $r\mid s$．

（ⅲ）$[B:k][C_A(B):k]=[A:k]$．

（ⅳ）$C_A(C_A(B))=B$．

证明 A 中乘法的结合性表明可以把 A 看作一个 (B,A)-双模．这样，它是一个左 $(B\otimes_k A^{\mathrm{op}})$-模，其中对一切 $x\in A$，$(b\otimes a)x=bxa$；我们记这个模为 A^*．但根据定理 9.112，$B\otimes_k A^{\mathrm{op}}$ 是单 k-代数，从而系 8.63 给出对某个整数 s 和某个域 k 上的可除代数 Δ 有 $B\otimes_k A^{\mathrm{op}}\cong\mathrm{Mat}_s(\Delta)$；事实上，$B\otimes_k A^{\mathrm{op}}$ 有唯一的（不计同构）极小左理想 L，且 $\Delta^{\mathrm{op}}\cong\mathrm{End}_{B\otimes_k A^{\mathrm{op}}}(L)$．所以，作为 $(B\otimes_k A^{\mathrm{op}})$-模，系 8.44 给出 $A^*\cong L^r$，即 L 的 r 个复制的直和，从而 $\mathrm{End}_{B\otimes_k A^{\mathrm{op}}}(A^*)\cong\mathrm{Mat}_r(\Delta^{\mathrm{op}})$．

我们断言

$$C_A(B)\cong\mathrm{End}_{B\otimes_k A^{\mathrm{op}}}(A^*)\cong\mathrm{Mat}_r(\Delta^{\mathrm{op}});$$

这就证明了（ⅰ）和（ⅱ）的大部分．如果 $\varphi\in\mathrm{End}_{B\otimes_k A^{\mathrm{op}}}(A^*)$，则特别地，它是 A 作为右 A-模的自同态．因此，对一切 $a\in A$，有

$$\varphi(a)=\varphi(1a)=\varphi(1)a=ua,$$

其中 $u=\varphi(1)$．特别地，如果 $b\in B$，则 $\varphi(b)=ub$．另一方面，考虑 B 的左作用，有 $\varphi(b)=\varphi(b1)=b\varphi(1)=bu$．所以对一切 $b\in B$ 有 $ub=bu$，从而 $u\in C_A(B)$．于是，$\varphi\mapsto\varphi(1)$ 是函数 $\mathrm{End}_{B\otimes_k A^{\mathrm{op}}}(A^*)\to C_A(B)$．容易验证这个函数是单射 k-代数映射；它也是满射，这是因为如果 $u\in C_A(B)$，则由 $a\mapsto ua$ 定义的映射 $A\to A$ 是 $(B\otimes_k A^{\mathrm{op}})$-映射．

731

我们现在计算维数．定义 $d=[\Delta:k]$．因 L 是 $\mathrm{Mat}_s(\Delta)$ 中的极小左理想，有 $\mathrm{Mat}_s(\Delta)\cong L^s$（具体地说，$L=\mathrm{COL}(1)$，它由 Δ 上 $s\times s$ 矩阵的第一列组成）．所以，$[\mathrm{Mat}_s(\Delta):k]=s^2[\Delta:k]$ 和 $[L^s:k]=s[L:k]$，从而

$$[L:k]=sd$$

和

$$[A:k]=[A^*:k]=[L^r:k]=rsd.$$

由此

$$[A:k][B:k]=[B\otimes_k A^{\text{op}}:k]=[\text{Mat}_s(\Delta):k]=s^2d.$$

所以，$[B:k]=\frac{s^2d}{rsd}=\frac{s}{r}$，从而 $r\mid s$. 因此，

$$[B:k][C_A(B):k]=[B:k][\text{Mat}_r(\Delta):k]=\frac{s}{r}\cdot r^2d=rsd=[A:k],$$

这是因为我们已经证明 $C_A(B)\cong\text{Mat}_r(\Delta)$.

最后，我们证明（ⅳ）. 易知 $B\subseteq C_A(C_A(B))$：毕竟，如果 $b\in B$ 和 $u\in C_A(B)$，则 $bu=ub$，从而 b 和每个这样的 u 可交换. 但根据（ⅰ），$C_A(B)$ 是单子代数，从而可以在（ⅲ）的等式中把 B 换成 $C_A(B)$：

$$[C_A(B):k][C_A(C_A(B)):k]=[A:k].$$

由此可知 $[B:k]=[C_A(C_A(B)):k]$；这个等式和 $B\subseteq C_A(C_A(B))$ 一起给出 $B=C_A(C_A(B))$. ■

下面是这个定理的一个小变动.

系 9.116 如果 B 是中心单 k-代数 A 的单子代数，其中 k 是域，则存在可除代数 D 使得 $B^{\text{op}}\otimes_k A\cong\text{Mat}_s(D)$.

证明 根据定理9.115（ⅱ），对某个可除代数 Δ 有 $B\otimes_k A^{\text{op}}\cong\text{Mat}_s(\Delta)$. 因此，$(B\otimes_k A^{\text{op}})^{\text{op}}\cong(\text{Mat}_s(\Delta))^{\text{op}}$. 但根据命题 8.13，$(\text{Mat}_s(\Delta))^{\text{op}}\cong\text{Mat}_s(\Delta^{\text{op}})$，而根据习题 9.65，$(B\otimes_k A^{\text{op}})^{\text{op}}\cong B^{\text{op}}\otimes_k A$. 令 $D=\Delta^{\text{op}}$ 即完成证明. ■

如果 Δ 是域 k 上的可除代数和 $\delta\in\Delta$，则由 k 和 δ 生成的子可除代数是域，这是因为中心 k 中的元素和 δ 可交换. 我们感兴趣的是 Δ 的极大子域.

引理 9.117 如果 Δ 是域 k 上的可除代数，则 Δ 的子域 E 是极大子域当且仅当 $C_\Delta(E)=E$.

证明 如果 E 是 Δ 的极大子域，则因 E 是交换的，所以 $E\subseteq C_\Delta(E)$. 关于反包含，易知如果 $\delta\in C_\Delta(E)$，则由 E 和 δ 生成的可除代数 E' 是域. 因此，如果 $\delta\notin E$，则 $E\subsetneq E'$，与 E 的极大性矛盾.

反之，假设 E 是满足 $C_\Delta(E)=E$ 的子域. 如果 E 不是 Δ 的极大子域，则存在子域 E' 使得 $E\subsetneq E'$. 现在 $E'\subseteq C_\Delta(E)$，因此如果有某个 $a'\in E'$ 而 $a'\notin E$，则 $E\neq C_\Delta(E)$. 所以 E 是极大子域. ■ 732

在证明了关于张量积的一个初等引理之后，我们要把下面的结果从可除代数推广到中心单代数（见定理 9.127）.

定理 9.118 如果 D 是域 k 上的可除代数和 E 是 D 的极大子域，则 E 是 D 的分裂域；即 $E\otimes_k D\cong\text{Mat}_s(E)$，其中 $s=[D:E]=[E:k]$.

证明 我们令定理 9.115 中的代数 $A=D, B=E$，根据引理 9.117，$C_A(E)=E$. 现在条件 $C_A(B)\cong\text{Mat}_r(\Delta)$ 变成 $E\cong\text{Mat}_r(\Delta)$；因 E 是交换的，$r=1$ 和 $\Delta=E$. 于是系 9.116 说 $E\otimes_k D=E^{\text{op}}\otimes_k D\cong\text{Mat}_s(E)$.

定理 9.115（ⅲ）中的等式现在是 $[D:k]=[E:k][E:k]=[E:k]^2$. 但 $[E\otimes_k D:k]=[\text{Mat}_s(E):k]=s^2[E:k]$，从而 $s^2=[D:k]=[E:k]^2$ 和 $s=[E:k]$. ■

系 9.119 如果 D 是域 k 上的可除代数，则一切极大子域在 k 上有相同的次数.

证明 对每个极大子域 E，有 $[E:k]=[D:E]=\sqrt{[D:k]}$. ■

这个系可以用例 9.113 来说明. 四元数$\mathbb{H}$是四维$\mathbb{R}$-代数，从而极大子域在$\mathbb{R}$上的次数必是 2. 因为$\mathbb{C}$是极大子域，所以确实如此.

我们现在证明一个技术性的定理，它会产生一个奇妙的结果. 回忆非交换环 A 中的一个单位是在 A 中有双边逆元的元素.

定理 9.120 设 k 是域，B 是单 k-代数，并设 A 是中心单 k-代数. 如果存在代数映射 f, $g: B\to A$，则存在单位 $u\in A$ 使得对一切 $b\in B$ 有

$$g(b)=uf(b)u^{-1}.$$

证明 如果定义 $b\in B$ 在元素 $a\in A$ 上的作用为 $f(b)a$，则 f 把 A 变成一个左 B-模. 因为 A 中的结合律对一切 $x\in A$ 给出，$(f(b)x)a=f(b)(xa)$，所以这个作用还把 A 变成一个 (B,A)-双模. 和通常一样，这个 (B,A)-双模是一个左 $(B\otimes_k A^{\mathrm{op}})$-模，其中对一切 $a\in A$ 有 $(b\otimes a')a=baa'$；把它记为 ${}_fA$. 类似地，可用 g 把 A 变成一个左 $(B\otimes_k A^{\mathrm{op}})$-模，把它记为 ${}_gA$. 根据定理 9.112, $B\otimes_k A^{\mathrm{op}}$ 是单 k-代数. 现在

733

$$[{}_fA:\Delta]=[A:\Delta]=[{}_gA:\Delta],$$

从而根据系 8.63，作为 $(B\otimes_k A^{\mathrm{op}})$-模，${}_fA\cong {}_gA$. 如果 $\varphi: {}_fA\to {}_gA$ 是 $(B\otimes_k A^{\mathrm{op}})$-同构，则对一切 $b\in B$ 和 a, $a'\in A$,

$$\varphi(f(b)aa')=g(b)\varphi(a)a'. \tag{4}$$

因 φ 是 A 作为它自身上的右模的自同构，有 $\varphi(a)=\varphi(1a)=ua$，其中 $u=\varphi(1)\in A$. 为证明 u 是单位，注意对一切 $a\in A$, $\varphi^{-1}(a)=u'a$. 现在对一切 $a\in A$, $a=\varphi\varphi^{-1}(a)=\varphi(u'a)=uu'a$；特别地，当 $a=1$ 时，有 $1=uu'$. 等式 $\varphi^{-1}\varphi=1_A$ 给出所要的 $1=u'u$. 代入等式 (4)，对一切 $a\in A$ 有

$$uf(b)a=\varphi(f(b)a)=g(b)\varphi(a)=g(b)ua.$$

特别地，如果 $a=1$，则 $uf(b)=g(b)u$ 和 $g(b)=uf(b)u^{-1}$. ■

系 9.121（斯科伦-诺特） 设 A 是域 k 上的中心单 k—代数，并设 B 和 B' 是 A 的同构的单 k-子代数. 如果 $\psi: B\to B'$ 是同构，则存在单位 $u\in A$ 使得对一切 $b\in B$ 有 $\psi(b)=ubu^{-1}$.

证明 在定理中取 $f: B\to A$ 为包含映射，定义 $B'=\mathrm{im}\psi$，并定义 $g=i\psi$，其中 $i: B'\to A$ 是包含映射. ■

在群论中有一个定理类似于斯科伦-诺特定理. G. Higman, B. H. Neumann 和 H. Neumann 的一个定理说，如果 B 和 B' 是群 G 的同构子群，比如 $\varphi: B\to B'$ 是同构，则存在包含 G 的群 G^* 和一个元素 $u\in G^*$ 使得对一切 $b\in B$ 有 $\varphi(b)=ubu^{-1}$. 在 Rotman 所著的《An Introduction to the Theory of Groups》404 页有一个证明.

系 9.122 设 k 是域. 如果 ψ 是 $\mathrm{Mat}_n(k)$ 的自同构，则存在非奇异矩阵 $P\in\mathrm{Mat}_n(k)$，对 $\mathrm{Mat}_n(k)$ 中的每个矩阵 T 有

$$\psi(T)=PTP^{-1}.$$

证明 矩阵环 $A=\mathrm{Mat}_n(k)$ 是中心单 k-代数. 在斯科伦-诺特定理中令 $B=B'=A$ 即可. ■

下面的韦德伯恩定理的证明属于范德瓦尔登 (B. L. van der Waerden).

定理 9.123（韦德伯恩） 每个有限可除环 D 都是域.

证明 设 $Z=Z(D)$，并设 E 是 D 的极大子域. 如果 $d\in D$，则 $Z(d)$ 是 D 的子域，因此存在极大子域 E_d 包含 $Z(d)$. 根据系 9.119，一切极大子域有相同的次数，因此有相同的阶. 根据系 3.132，这里的一切极大子域都同构.[⊖] 对每个 $d\in D$，斯科伦-诺特定理说存在 $x_d\in D$ 使得 $E_d=x_dEx_d^{-1}$. 所以，$D=\bigcup_x xEx^{-1}$，从而

734

$$D^{\times}=\bigcup_x xE^{x}x^{-1}.$$

如果 E 是 D 的真子域，则 $E^{\times}$ 是 $D^{\times}$ 的真子群，因此这个等式和习题 5.32 矛盾. 所以，$D=E$ 是交换的. ■

定理 9.124（弗罗贝尼乌斯） *如果 D 是非交换的有限维实可除代数，则 $D\cong\mathbb{H}$.*

证明 如果 E 是 D 的极大子域，则 $[D:E]=[E:\mathbb{R}]\leqslant 2$. 如果 $[E:\mathbb{R}]=1$，则 $[D:\mathbb{R}]=1^2=1$ 和 $D=\mathbb{R}$. 因此，$[E:\mathbb{R}]=2$ 和 $[D:\mathbb{R}]=4$. 我们把 E 等同于$\mathbb{C}$（它们同构）. 现在复共轭是 E 的一个自同构，从而斯科伦-诺特定理给出 $x\in D$ 使得对一切 $z\in E$ 有 $\bar{z}=xzx^{-1}$. 特别地，$-\mathrm{i}=x\mathrm{i}x^{-1}$. 因此，

$$x^2\mathrm{i}x^{-2}=x(-\mathrm{i})x^{-1}=-x\mathrm{i}x^{-1}=\mathrm{i}.$$

从而 x^2 和 i 可交换. 所以，根据引理 9.117，$x^2\in C_D(E)=E$，因此有 a，$b\in\mathbb{R}$ 使得 $x^2=a+b\mathrm{i}$. 但

$$a+b\mathrm{i}=x^2=xx^2x^{-1}=x(a+b\mathrm{i})x^{-1}=a-b\mathrm{i},$$

因此 $b=0$ 和 $x^2\in\mathbb{R}$. 如果 $x^2>0$，则存在 $t\in\mathbb{R}$ 使得 $x^2=t^2$. 现在 $(x+t)(x-t)=0$ 给出 $x=\pm t\in\mathbb{R}$，与 $-\mathrm{i}=x\mathrm{i}x^{-1}$ 矛盾. 所以有某个实数 r 使得 $x^2=-r^2$. 定义元素 $j=x/r$，j 满足 $j^2=-1$ 和 $j\mathrm{i}=-\mathrm{i}j$. 表 $1,\mathrm{i},j,\mathrm{i}j$ 在$\mathbb{R}$上线性无关：如果 $a+b\mathrm{i}+cj+d\mathrm{i}j=0$，则 $(-d\mathrm{i}-c)j=a+\mathrm{i}b\in\mathbb{C}$. 因 $j\notin\mathbb{C}$（否则 $x\in\mathbb{C}$），必有 $-d\mathrm{i}-c=0=a+b\mathrm{i}$. 因此，$a=b=0=c=d$. 由于$[D:\mathbb{R}]=4$，表 $1,\mathrm{i},j,\mathrm{i}j$ 是 D 的基. 现在容易知道，如果定义 $k=\mathrm{i}j$，则 $k\mathrm{i}=j=-\mathrm{i}k, jk=\mathrm{i}=-kj$ 和 $k^2=-1$，因此 $D\cong\mathbb{H}$. ■

1929 年，布饶尔引入布饶尔群来研究除环. 因除环的构造极其困难，他考虑了更广的中心单代数类. 布饶尔引入了中心单 k-代数上的下面的关系.

定义 *如果对于两个中心单 k-代数 A 和 B，存在整数 n 和 m 使得*

$$A\otimes_k \mathrm{Mat}_n(k)\cong B\otimes_k \mathrm{Mat}_m(k),$$

则称 A 和 B **相似**，*记为 $A\sim B$.*

根据韦德伯恩定理，有 k 上唯一的可除代数Δ 使得$A\cong\mathrm{Mat}_n(\Delta)$，我们将看到 $A\sim B$ 当且仅当它们确定相同的可除代数.

735

引理 9.125 *设 A 是域k 上的有限维代数. 如果 S 和 T 是 A 的 k-子代数满足*

（i）对一切 $s\in S$ 和 $t\in T, st=ts$；

（ii）$A=ST$；

（iii）$[A:k]=[S:k][T:k]$.

则 $A\cong S\otimes_k T$.

证明 因为 $(s,t)\mapsto st$ 是 k-双线性函数 $S\times T\to A$，所以存在 $s\otimes t\mapsto st$ 的 k-线性变换 $f:S\otimes_k T\to A$. 条件（i）蕴涵 f 是代数映射，这是因为

⊖ 并非任意可除代数中的极大子域都同构，见习题 9.80.

$$f((s\otimes t)(s'\otimes t'))=f(ss'\otimes tt')=ss'tt'=sts't'=f(s\otimes t)f(s'\otimes t').$$

根据条件（ⅱ），因 $A=ST$，从而 k-线性变换 f 是满射；根据条件（ⅲ），因 $\dim_k(S\otimes_k T)=\dim_k(A)$，因此 f 是 k-代数同构． ■

引理 9.126 设 k 是域．

（ⅰ）如果 A 是 k-代数，则

$$A\otimes_k \mathrm{Mat}_n(k)\cong \mathrm{Mat}_n(A).$$

（ⅱ）$\mathrm{Mat}_n(k)\otimes_k \mathrm{Mat}_m(k)\cong \mathrm{Mat}_{nm}(k)$．

（ⅲ）$A\sim B$ 是一个等价关系．

（ⅳ）如果 A 是中心单代数，则

$$A\otimes_k A^{\mathrm{op}}\cong \mathrm{Mat}_n(k),$$

其中 $n=[A:k]$．

证明 （ⅰ）定义 $\mathrm{Mat}_n(A)$ 的 k-子代数为

$$S=\mathrm{Mat}_n(k)\text{ 和 }T=\{aI:a\in A\}.$$

如果 $s\in S$ 和 $t\in T$，则 $st=ts$（因为 S 中矩阵的元素和元素 $a\in A$ 可交换）．现在 S 包含每个矩阵单位 E_{ij}（ij 元素为 1 其他元素为 0)，从而对一切 ij，ST 包含一切形如 $a_{ij}E_{ij}$ 的矩阵，其中 $a_{ij}\in A$；因此 $ST=\mathrm{Mat}_n(A)$．最后，$[S:k][T:k]=n^2[A:k]=[\mathrm{Mat}_n(A):k]$．所以，引理 9.125 给出所要的同构．

（ⅱ）如果 V 和 W 分别是域 k 上 n 维和 m 维向量空间，只要证明 $\mathrm{End}_k(V)\otimes_k \mathrm{End}_k(W)\cong \mathrm{End}_k(V\otimes_k W)$．定义 S 为一切 $f\otimes 1_W$，其中 $f\in \mathrm{End}_k(V)$，并定义 T 为一切 $1_V\otimes g$，其中 $g\in \mathrm{End}_k(W)$．容易验证引理 9.125 中的三个条件成立．

736

（ⅲ）因 $k=\mathrm{Mat}_1(k)$，我们有 $A\cong A\otimes_k k\cong A\otimes_k \mathrm{Mat}_1(k)$，因此～是自反的．对称性是显然的；关于传递性，假设 $A\sim B$ 和 $B\sim C$；即

$$A\otimes_k \mathrm{Mat}_n(k)\cong B\otimes_k \mathrm{Mat}_m(k)\text{ 和 }B\otimes_k \mathrm{Mat}_r(k)\cong C\otimes_k \mathrm{Mat}_s(k).$$

则根据（ⅱ），$A\otimes_k \mathrm{Mat}_n(k)\otimes_k \mathrm{Mat}_r(k)\cong A\otimes_k \mathrm{Mat}_{nr}(k)$．另一方面，

$$\begin{aligned}A\otimes_k \mathrm{Mat}_n(k)\otimes_k \mathrm{Mat}_r(k)&\cong B\otimes_k \mathrm{Mat}_m(k)\otimes_k \mathrm{Mat}_r(k)\\&\cong C\otimes_k \mathrm{Mat}_m(k)\otimes_k \mathrm{Mat}_s(k)\\&\cong C\otimes_k \mathrm{Mat}_{ms}(k).\end{aligned}$$

所以，$A\sim C$，从而 ～ 是等价关系．

（ⅳ）定义 $f:A\times A^{\mathrm{op}}\to \mathrm{End}_k(A)$ 为 $f(a,c)=\lambda_a\circ\rho_c$，其中 $\lambda_a:x\mapsto ax$ 和 $\rho_c:x\mapsto xc$；容易验证 λ_a 和 ρ_c 都是 k-映射(从而它们的复合也是 k-映射)，且 f 是 k-双加性的．因此，存在 $\hat f(a\otimes c)=\lambda_a\circ\rho_c$ 的 k-映射 $\hat f:A\otimes_k A^{\mathrm{op}}\to \mathrm{End}_k(A)$．$A$ 中的结合性 $a(xc)=(ax)c$ 说明 $\lambda_a\circ\rho_c=\rho_c\circ\lambda_a$，由此易知 $\hat f$ 是 k-代数映射．因 $A\otimes_k A^{\mathrm{op}}$ 是单 k-代数和 $\ker\hat f$ 是真双边理想，所以 $\hat f$ 是单射．现在 $\dim_k(\mathrm{End}_k(A))=\dim_k(\mathrm{Hom}_k(A,A))=n^2$，其中 $n=[A:k]$．因 $\dim_k(\mathrm{im}\hat f)=\dim_k(A\otimes_k A^{\mathrm{op}})=n^2$，从而 $\hat f$ 是 k-代数同构：$A\otimes_k A^{\mathrm{op}}\cong \mathrm{End}_k(A)$． ■

我们现在把定理 9.118 从可除代数扩展到中心单代数．

定理 9.127 设 A 是域 k 上的中心单 k-代数，从而 $A\cong \mathrm{Mat}_r(\Delta)$，其中 Δ 是域 k 上的可除代数．如果 E 是 Δ 的极大子域，则 E 分裂 A；即存在整数 n 和同构

$$E\otimes_k A\cong \mathrm{Mat}_n(E).$$

精确地说，如果 $[\Delta:E]=s$，则 $n=rs$ 和$[A:k]=(rs)^2$.

证明 根据定理 9.118，Δ 被极大子域 E 分裂（当然，E 是 k 的有限扩张）：$E\otimes_k\Delta\cong\mathrm{Mat}_s(E)$，其中 $s=[\Delta:E]=[E:k]$. 因此

$$E\otimes_k A\cong E\otimes_k\mathrm{Mat}_r(\Delta)\cong E\otimes_k(\Delta\otimes_k\mathrm{Mat}_r(k))$$
$$\cong(E\otimes_k\Delta)\otimes_k\mathrm{Mat}_r(k)\cong\mathrm{Mat}_s(E)\otimes_k\mathrm{Mat}_r(k)\cong\mathrm{Mat}_{rs}(E).$$

所以，$A\cong\mathrm{Mat}_r(\Delta)$ 给出 $[A:k]=r^2[\Delta:k]=r^2s^2$. ■

定义 如果 $[A]$ 表示中心单 k-代数 A 在相似性下的等价类，定义**布饶尔群** $\mathrm{Br}(k)$为集合

$$\mathrm{Br}(k)=\{[A]:A\text{ 是中心单 }k\text{-代数}\},$$

它有二元运算

$$[A][B]=[A\otimes_k B].$$

737

定理 9.128 对每个域 k，$\mathrm{Br}(k)$ 是阿贝尔群. 此外，如果有可除代数 Δ 使得 $A\cong\mathrm{Mat}_n(\Delta)$，则 Δ 是中心单 k-代数且在 $\mathrm{Br}(k)$ 中 $[A]=[\Delta]$.

证明 我们证明运算是合理定义的：如果 A，A'，B，B' 是 k-代数且 $A\sim A'$和 $B\sim B'$，则 $A\otimes_k B\sim A'\otimes_k B'$. 同构

$$A\otimes_k\mathrm{Mat}_n(k)\cong A'\otimes_k\mathrm{Mat}_m(k)\text{ 和 }B\otimes_k\mathrm{Mat}_r(k)\cong B'\otimes_k\mathrm{Mat}_s(k)$$

给出 $A\otimes_k B\otimes_k\mathrm{Mat}_n(k)\otimes_k\mathrm{Mat}_r(k)\cong A'\otimes_k B'\otimes_k\mathrm{Mat}_m(k)\otimes_k\mathrm{Mat}_s(k)$（用到了张量积的交换性和结合性），从而引理 9.126（ⅱ）给出 $A\otimes_k B\otimes_k\mathrm{Mat}_{nr}(k)\cong A'\otimes_k B'\otimes_k\mathrm{Mat}_{ms}(k)$. 所以，$A\otimes_k B\sim A'\otimes_k B'$.

由 $k\otimes_k A\cong A$ 可知 $[k]$ 是幺元，结合性和交换性来自张量积的结合性和交换性，引理9.126(ⅳ)证明 $[A]^{-1}=[A^{\mathrm{op}}]$. 所以，$\mathrm{Br}(k)$ 是阿贝尔群.

如果 A 是中心单 k-代数，则有 k 上的某个有限维可除代数 Δ 使得 $A\cong\mathrm{Mat}_r(\Delta)$. 因此根据定理 9.112，$k=Z(A)\cong Z(\mathrm{Mat}_r(\Delta))\cong Z(\Delta)$. 于是，$\Delta$ 是中心单 k-代数，$[\Delta]\in\mathrm{Br}(k)$ 且$[\Delta]=[A]$（因为 $\Delta\otimes_k\mathrm{Mat}_r(k)\cong\mathrm{Mat}_r(\Delta)\cong A\cong A\otimes_k k\cong A\otimes_k\mathrm{Mat}_1(k)$）. ■

下一命题表明布饶尔群的重要性.

命题 9.129 如果 k 是域，则存在从 $\mathrm{Br}(k)$ 到域 k 上有限维可除代数的一切同构类的族$\mathcal{D}$的双射，从而 $|\mathrm{Br}(k)|=|\mathcal{D}|$. 因此，存在非交换除环，该环在它的中心 k 上是有限维的，当且仅当 $\mathrm{Br}(k)\neq\{0\}$.

证明 定义函数 $\varphi:\mathrm{Br}(k)\to\mathcal{D}$ 为如果 $A\cong\mathrm{Mat}_n(\Delta)$，则 $\varphi([A])$ 是 Δ 的同构类. 注意定理 9.128 证明在 $\mathrm{Br}(k)$ 中$[A]=[\Delta]$. 我们证明 φ 是合理定义的. 如果$[\Delta]=[\Delta']$，则 $\Delta\sim\Delta'$，从而存在整数 n 和 m 使得 $\Delta\otimes_k\mathrm{Mat}_n(k)\cong\Delta'\otimes_k\mathrm{Mat}_m(k)$. 因此，$\mathrm{Mat}_n(\Delta)\cong\mathrm{Mat}_m(\Delta')$. 由韦德伯恩-阿廷定理中的唯一性，$\Delta\cong\Delta'$（和 $n=m$）. 所以，$\varphi([\Delta])=\varphi([\Delta'])$.

显然 φ 是满射，这是因为如果 Δ 是 k 上的有限维可除代数，则 Δ 的同构类等于 $\varphi([\Delta])$. 为证明 φ 是单射，假设 $\varphi([\Delta])=\varphi([\Delta'])$. 则 $\Delta\cong\Delta'$，这蕴涵 $\Delta\sim\Delta'$. ■

例 9.130 （ⅰ）如果 k 是代数闭域，则定理 9.114 表明 $\mathrm{Br}(k)=\{0\}$.

（ⅱ）如果 k 是有限域，则韦德伯恩的定理 9.123（=定理 8.23）表明 $\mathrm{Br}(k)=\{0\}$.

（ⅲ）如果 $k=\mathbb{R}$，则弗罗贝尼乌斯的定理 9.124 表明 $\mathrm{Br}(\mathbb{R})\cong\mathbb{I}_2$.

（ⅳ）用类域定理可证明 $\mathrm{Br}(\mathbb{Q}_p)\cong\mathbb{Q}/\mathbb{Z}$，其中$\mathbb{Q}_p$ 是 p-进位数的域. 此外，存在正合列

$$0\to\mathrm{Br}(\mathbb{Q})\to\mathrm{Br}(\mathbb{R})\oplus\sum_p\mathrm{Br}(\mathbb{Q}_p)\xrightarrow{\varphi}\mathbb{Q}/\mathbb{Z}\to 0.$$

738

如果记 $\mathrm{Br}(\mathbb{R})=\langle\frac{1}{2}+\mathbb{Z}\rangle\subseteq\mathbb{Q}/\mathbb{Z}$，则 φ 是“坐标和”映射.

在一系列深入研究的论文中，阿尔伯特（A. A. Albert）、布饶尔、哈塞和诺特对代数数论引发的最重要的域 k（局部域（$\mathbb{Q}_p$ 是其中之一）和整体域）计算了 $\mathrm{Br}(k.)$ ■

命题 9.131 *如果 E/k 是域扩张，则 $[A]\mapsto[E\otimes_k A]$ 给出同态*

$$f_{E/k}:\mathrm{Br}(k)\to\mathrm{Br}(E).$$

证明 如果 A 和 B 是中心单 k-代数，根据定理 9.112，$E\otimes_k A$ 和 $E\otimes_k B$ 是中心单 E-代数. 如果 $A\sim B$，则根据习题 9.77，作为 E-代数有 $E\otimes_k A\sim E\otimes_k B$. 由此函数 $f_{E/k}$ 是合理定义的. 最后，根据命题 8.84，即张量积的结合性，有

$$(E\otimes_k A)\otimes_E(E\otimes_k B)\cong(E\otimes_E E)\otimes_k(A\otimes_k B)\cong E\otimes_k(A\otimes_k B),$$

因此 $f_{E/k}$ 是同态. ■

定义 *如果 E/k 是域扩张，则***相对布饶尔群** $\mathrm{Br}(E/k)$ *是指同态 $f_{E/k}:\mathrm{Br}(k)\to\mathrm{Br}(E)$ 的核：*

$$\mathrm{Br}(E/k)=\ker f_{E/k}=\{[A]\in\mathrm{Br}(k):A\text{ 被 }E\text{ 分裂}\}.$$

系 9.132 *对每个域 k，有*

$$\mathrm{Br}(k)=\bigcup_{E/k\text{有限}}\mathrm{Br}(E/k).$$

证明 由定理 9.127 立即可得. ■

简而言之，布饶尔群作为研究除环的一种方法而产生. 它是一个重要的对象，但我们还没有认真的运用它. 例如，一直以来我们只知道除了实可除代数 $\mathbb{H}$ 和它关于 $\mathbb{R}$ 的子域 k 的变种之外没有其他的非交换除环. 在第 10 章中引入叉积代数后我们会弥补这一点. 例如，在系 10.133 中会看到存在这样的除环，它的中心是特征为 $p>0$ 的域. 关于进一步的阐述，读者可参考 Jacobson 所著的《Finite-Dimensional Division Algebra over Fields》和 Reiner 所著的《Maximal Orders》.

739

习题

9.72 证明作为 $\mathbb{R}$-代数，$\mathbb{H}\otimes_{\mathbb{R}}\mathbb{H}\cong\mathrm{Mat}_4(\mathbb{R})$.

提示：对中心单 $\mathbb{R}$-代数 $\mathbb{H}\otimes_{\mathbb{R}}\mathbb{H}$ 用系 8.60.

9.73 例 9.113 中已经给出一个同构 $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{H}\cong\mathrm{Mat}_2(\mathbb{C})$. 描述这两个代数之间的一切可能的同构.

提示：用斯科伦-诺特定理.

9.74 证明作为 $\mathbb{R}$-代数，$\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}\cong\mathbb{C}\times\mathbb{C}$.

9.75 (i) 设 $\mathbb{C}(x)$ 和 $\mathbb{C}(y)$ 是函数域. 证明 $R=\mathbb{C}(x)\otimes_{\mathbb{C}}\mathbb{C}(y)$ 同构于 $\mathbb{C}(x,y)$ 的一个子环. 由此推出 R 没有零因子.

(ii) 证明 $\mathbb{C}(x)\otimes_{\mathbb{C}}\mathbb{C}(y)$ 不是域.

提示：证明 R 同构于 $\mathbb{C}(x,y)$ 的一个由形如 $f(x,y)/g(x)h(y)$ 的多项式组成的子环.

(iii) 用习题 8.39 证明阿廷代数的张量积未必是阿廷代数.

9.76 设 A 是中心单 k-代数. 如果 A 被域 E 分裂，证明 A 被 E 的任一域扩张 E' 分裂.

9.77 设 E/k 是域扩张. 如果 A 和 B 是中心单 k-代数，且 $A\sim B$. 证明作为中心单 E-代数有 $E\otimes_k A\sim E\otimes_k B$.

9.78 如果 D 是 $\mathbb{R}$ 上的有限维可除代数，证明 D 同构于 $\mathbb{R}$，$\mathbb{C}$ 或 $\mathbb{H}$.

9.79 证明作为 $\mathbb{R}$-代数，$\mathrm{Mat}_2(\mathbb{H})\cong\mathbb{H}\otimes_{\mathbb{R}}\mathrm{Mat}_2(\mathbb{R})$.

9.80 (i) 设 A 是$\mathbb{Q}$上的四维向量空间，并设$1,i,j,k$是基. 如果定义 1 为幺元且

$$\begin{array}{lll} i^2=-1 & j^2=-2 & k^2=-2 \\ ij=k & jk=2i & ki=j \\ ji=-k & kj=-2i & ik=-j \end{array}$$

证明 A 是$\mathbb{Q}$上的可除代数.

(ii) 证明$\mathbb{Q}(i)$ 和$\mathbb{Q}(j)$ 是 A 的不同构的极大子域.

9.81 设 D 是$\mathbb{H}$ 的$\mathbb{Q}$-子代数且有基$1,i,j,k$.

(i) 证明 D 是$\mathbb{Q}$上的可除代数.

提示：计算中心 $Z(D)$.

(ii) 对任意一对非零有理数 p 和 q，证明 D 有极大子域同构于$\mathbb{Q}(\sqrt{-p^2-q^2})$.

提示：计算 $(pi+qj)^2$.

9.82 (**迪克森**) 如果 D 是域 k 上的可除代数，则每个 $d\in D$ 都是 k 上的代数元素. 证明 d，$d'\in D$ 在 D 中共轭当且仅当 $\mathrm{irr}(d,k)=\mathrm{irr}(d',k)$.

提示：用斯科伦-诺特定理.

9.83 证明：如果 A 是中心单 k-代数且 $A\sim\mathrm{Mat}_n(k)$，则有某个整数 m 使得 $A\cong\mathrm{Mat}_m(k)$. [740]

9.84 证明：如果 A 是中心单 k-代数且 $[A]$ 在 $\mathrm{Br}(k)$中有有限阶 m，则有某个整数 r 使得

$$A\otimes_k\cdots\otimes_k A\cong\mathrm{Mat}_r(k)$$

(有等于 A 的 m 个因子). (在第 10 章中，我们将看到 $\mathrm{Br}(k)$中每个元素的阶都有限.)

9.8 外代数

在微积分中，可微函数 $f(x,y)$在点 $P=(x_0,y_0)$处的**微分** $\mathrm{d}f$ 定义为

$$\mathrm{d}f\,|_P=\frac{\partial f}{\partial x}\,|_P(x-x_0)+\frac{\partial f}{\partial y}\,|_P(y-y_0).$$

如果 (x,y) 是邻近 P 的点，则 $\mathrm{d}f\,|_P$ 近似于 $f(x,y)$ 和 $f(x_0,y_0)$ 的真值之差. $\mathrm{d}f$ 被认为是一个"小"量，从而它的平方（即二阶近似）看作是可忽略的. 此刻，我们认真对待这个可忽略的量：假设对一切微分 $\mathrm{d}f$，

$$(\mathrm{d}f)^2\approx 0.$$

有一个不寻常的推论：如果 $\mathrm{d}u$ 和 $\mathrm{d}v$ 都是微分，则 $\mathrm{d}u+\mathrm{d}v=\mathrm{d}(u+v)$ 也是微分. 但 $(\mathrm{d}u+\mathrm{d}v)^2\approx 0$ 给出

$$\begin{aligned} 0 &\approx (\mathrm{d}u+\mathrm{d}v)^2 \\ &\approx (\mathrm{d}u)^2+\mathrm{d}u\mathrm{d}v+\mathrm{d}v\mathrm{d}u+(\mathrm{d}v)^2 \\ &\approx \mathrm{d}u\mathrm{d}v+\mathrm{d}v\mathrm{d}u, \end{aligned}$$

从而 $\mathrm{d}u$ 和 $\mathrm{d}v$ 反交换：

$$\mathrm{d}v\mathrm{d}u\approx-\mathrm{d}u\mathrm{d}v.$$

现在考虑二重积分 $\iint_D f(x,y)\mathrm{d}x\mathrm{d}y$，其中 D 是平面上的某个区域. 等式

$$\begin{aligned} x &= F(u,v) \\ y &= G(u,v) \end{aligned}$$

导出变量替换公式：

$$\iint_D f(x,y)\mathrm{d}x\mathrm{d}y=\iint_\Delta f(F(u,v),G(u,v))J\mathrm{d}u\mathrm{d}v,$$

其中 Δ 是某个新区域且 J 是雅可比行列式

741

$$J=\left|\det\begin{bmatrix}F_u & F_v\\ G_u & G_v\end{bmatrix}\right|.$$

证明这个公式的关键思想是把可微函数 $f(x,y)$的图像局部地看作一个实向量空间——它的切平面.我们记一点的切平面的基为 $\mathrm{d}x,\mathrm{d}y$. 如果 $\mathrm{d}u,\mathrm{d}v$ 是这个切平面的另外一组基，则链式法则由下面的线性方程组：

$$\begin{aligned}\mathrm{d}x &= F_u\mathrm{d}u+F_v\mathrm{d}v\\ \mathrm{d}y &= G_u\mathrm{d}u+G_v\mathrm{d}v\end{aligned}$$

定义了一个线性变换．现在自然地产生雅可比行列式.

$$\begin{aligned}\mathrm{d}x\mathrm{d}y &= (F_u\mathrm{d}u+F_v\mathrm{d}v)(G_u\mathrm{d}u+G_v\mathrm{d}v)\\ &= F_u\mathrm{d}uG_u\mathrm{d}u+F_u\mathrm{d}_uG_v\mathrm{d}v+F_v\mathrm{d}vG_u\mathrm{d}u+F_v\mathrm{d}vG_v\mathrm{d}v\\ &= F_uG_u(\mathrm{d}u)^2+F_uG_v\mathrm{d}u\mathrm{d}v+F_vG_u\mathrm{d}v\mathrm{d}u+F_vG_v(\mathrm{d}v)^2\\ &\approx F_uG_v\mathrm{d}u\mathrm{d}v+F_vG_u\mathrm{d}v\mathrm{d}u\\ &\approx (F_uG_v-F_vG_u)\mathrm{d}u\mathrm{d}v\\ &= \det\begin{bmatrix}F_u & F_v\\ G_u & G_v\end{bmatrix}\mathrm{d}u\mathrm{d}v.\end{aligned}$$

涉及方向的分析研究迫使我们在证明变量替换公式时使用这个行列式的绝对值．

在上面的等式中我们使用了分配律和结合律以及反交换性；即假定微分形成一个环，其中一切平方都是 0. 下面的构造把这种推断建立在一个坚实的基础之上．

定义 如果 M 是 k-模，其中 k 是交换环，则它的**外代数**[⊖]是指$\bigwedge(M)=T(M)/J$，读作“楔 M”，其中 J 是由一切满足 $m\in M$ 的 $m\otimes m$ 生成的双边理想. $m_1\otimes\cdots\otimes m_p$ 在$\bigwedge(M)$中的象记为

$$m_1\wedge\cdots\wedge m_p.$$

注意 J 是由齐次元素（2 次）生成的，从而根据命题 9.95，它是分次理想．因此，$\bigwedge(M)$ 是分次 k-代数，

$$\bigwedge(M)=k\oplus M\oplus\bigwedge^2(M)\oplus\bigwedge^3(M)\oplus\cdots,$$

其中对 $p\geqslant 2$，有$\bigwedge^p(M)=T^p(M)/J^p$, $J^p=J\cap T^p(M)$. 最后，$\bigwedge(M)$ 作为 k-代数由$\bigwedge^1(M)=M$ 生成.

742

定义 称$\bigwedge^p(M)$为 k-模 M 的 **p 次外幂**.

引理 9.133 设 k 是交换环，并设 M 是 k-模．

(i) 如果 $m,m'\in M$，则在$\bigwedge^2(M)$ 中，有

$$m\wedge m'=-m'\wedge m.$$

(ii) 如果 $p\geqslant 2$ 且有某个 $i\neq j$ 使得 $m_i=m_j$，则在$\bigwedge^p(M)$ 中有 $m_1\wedge\cdots\wedge m_p=0$.

⊖ 这里原先的形容词——意为“外面的”德语 ausserer——是格拉斯曼于 1844 年引入的．格拉斯曼用它和内积对比．第一次使用 exterior（外）的翻译可以在 1945 年嘉当的工作中找到，他说他是用了凯勒（Kaehler）的术语．楔形记号似乎是布尔巴基（Bourbaki）引入的．

证明 （ⅰ）回忆 $\bigwedge^2(M)=(M\otimes_k M)/J^2$，其中 $J^2=J\cap(M\otimes_k M)$．如果 $m,m'\in M$，则

$$(m+m')\otimes(m+m')=m\otimes m+m\otimes m'+m'\otimes m+m'\otimes m'.$$

因为 J^2 包含 $(m+m')\otimes(m+m')$，$m\otimes m$ 和 $m'\otimes m'$，所以，

$$m\otimes m'+J^2=-m'\otimes m+J^2,$$

由此对一切 m，$m'\in M$，

$$m\wedge m'=-m'\wedge m.$$

（ⅱ）和在命题 9.95 的证明中看到的一样，$\bigwedge^p(M)=T^p(M)/J^p$，其中 $J^p=J\cap T^p(M)$ 由理想 J 中的一切 p 次元素组成，而 J 由 $T^2(M)$ 中一切形如 $m\otimes m$ 的元素组成．详细地说，J^p 由齐次元素 $\alpha\otimes m\otimes m\otimes\beta$ 的一切和组成，其中 $m\in M,\alpha\in T^q(M),\beta\in T^r(M)$ 且 $q+r+2=p$；由此，如果有两个相邻因子相等，比如 $m_i=m_{i+1}$，则 $m_1\wedge\cdots\wedge m_p=0$．然而，因为 $\bigwedge(M)$ 中的乘法是结合的，我们可以（反）交换 $m_1\wedge\cdots\wedge m_p$ 中的一个因子 m_i 若干次，只是可能要变号，从而可以使得任意一对因子变成相邻的． ■

我们的目的之一是给出行列式的一个“无基础”的构造，这个思想是关注这种函数所应具备的一些性质．如果把 $n\times n$ 矩阵 A 看作由它的 n 个列组成，则它的行列式 $\det(A)$ 是 n 个变量（每一个排成 n 元组）的函数．行列式的一个性质是如果 A 的两列相等，则 $\det(A)=0$，另一个性质是它是多重线性的．我们将看到这两个性质几乎刻画了行列式．

定义 如果 M 和 N 都是 k-模，一个 k-多重线性函数 $f:\times^p M\to N$（其中 $\times^p M$ 是 p 个 M 的笛卡儿积）如果满足下列性质：一旦对某个 $i\neq j$ 有 $m_i=m_j$，就有

$$f(m_1,\cdots,m_p)=0,$$

则称 f 是**交错的**．

当考虑平面 $\mathbb{R}^2$ 中的（带符号的）面积时，自然地产生了交错 $\mathbb{R}$-双线性函数．如果 $v_1,v_2\in\mathbb{R}^2$，定义 $A(v_1,v_2)$ 为以 v_1 和 v_2 为边的平行四边形的面积．显然，对一切 $r,s\in\mathbb{R}$，

$$A(rv_1,sv_2)=rsA(v_1,v_2)$$

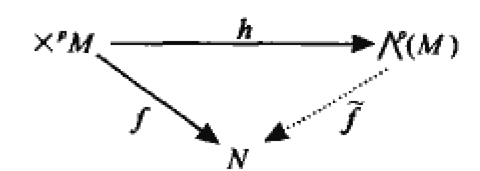
743

（但必须说明当这些数为负时是什么意思），用几何论证可以证明

$$A(w_1+v_1,v_2)=A(w_1,v_2)+A(v_1,v_2);$$

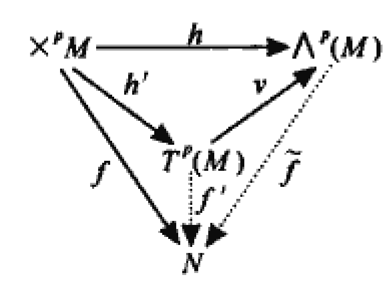
即 A 是 $\mathbb{R}$-双线性的．现在因为以 v_1 和 v_1 为边的退化“平行四边形”面积为零，因此 $A(v_i,v_i)=0$，所以 A 是交错的．类似的论证证明体积是 $\mathbb{R}^3$ 上的交错 $\mathbb{R}$-多重线性函数，这和我们在使用叉积的向量微积分中看到的一样．

定理 9.134 对一切 $p\geq 0$ 和一切 k-模 M，p 次外幂 $\bigwedge^p(M)$ 是由交错多重线性函数提出的泛映射问题的解．



如果 $h:\times^p M\to\bigwedge^p(M)$ 由 $h(m_1,\cdots,m_p)=m_1\wedge\cdots\wedge m_p$ 定义，则对每个交错多重线性函数 f，存在唯一的 k-同态 $\widetilde{f}$ 使得图交换．

证明 考虑图



其中 $h'(m_1,\cdots,m_p)=m_1\otimes\cdots\otimes m_p$ 和 $v(m_1\otimes\cdots\otimes m_p)=m_1\wedge\cdots\wedge m_p$．因 f 是多重线性的，存在 k-映射 $f':T^p(M)\to N$ 使得 $f'h'=f$；因 f 是交错的，$J\cap T^p(M)\subseteq \ker f'$，从而 f' 诱导出映射

$$\tilde{f}:T^p(M)/(J\cap T^p(M))\to N$$

使得 $\tilde{f}v=f'$．因此，

$$\tilde{f}h=\tilde{f}vh'=f'h'=f.$$

但 $T^p(M)/(J\cap T^p(M))=\bigwedge^p(M)$，这正是所要的．最后，因为 $\mathrm{im}h$ 生成 $\bigwedge^p(M)$，所以 $\tilde{f}$ 是唯一的这种映射． ■

744

命题 9.135 对每个 $p\geqslant 0$，p 次外幂是函子

$$\bigwedge^p:{}_k\mathbf{Mod}\to{}_k\mathbf{Mod}.$$

证明 现在 $\bigwedge^p(M)$ 已经定义在模上；剩下要在态射上定义它．假设 $g:M\to M'$ 是 k-同态．考虑图

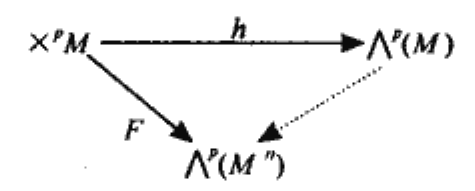
$\times^p M \xrightarrow{h} \bigwedge^p(M)$，$f$，$\bigwedge^p(g)$，$\bigwedge^p(M')$

其中 $f(m_1,\cdots,m_p)=gm_1\wedge\cdots\wedge gm_p$．易知 f 是交错多重线性函数，从而泛性产生唯一映射

$$\bigwedge^p(g):\bigwedge^p(M)\to\bigwedge^p(M')$$

使得 $m_1\wedge\cdots\wedge m_p\mapsto gm_1\wedge\cdots\wedge gm_p$．

如果 g 是模 M 上的恒等映射，则 $\bigwedge^p(g)$ 也是恒等映射，这是因为它固定生成元的集合．最后，假设 $g':M'\to M''$ 是 k-映射．容易验证 $\bigwedge^p(g'g)$ 和 $\bigwedge^p(g')\bigwedge^p(g)$ 使得下图交换：



其中 $F(m_1,\cdots,m_p)=g'gm_1\wedge\cdots\wedge g'gm_p$．这种虚线箭头的唯一性给出所要的 $\bigwedge^p(g'g)=\bigwedge^p(g')\bigwedge^p(g)$． ■

我们很快会看到 $\bigwedge^p$ 不如 Hom 或张量那样好，因为它不是加性函子．

定理 9.136 (反交换性) 如果 M 是 k-模，$x\in\bigwedge^p(M)$，$y\in\bigwedge^q(M)$，则

$$x\wedge y=(-1)^{pq}y\wedge x.$$

注 这个恒等式只对齐次元素的积成立．

证明 如果 $x\in\bigwedge^0(M)=k$，则$\bigwedge(M)$ 是 k-代数蕴涵对一切 $y\in\bigwedge(M)$，$x\wedge y=y\wedge x$，从而恒等式成立，特别对 $y\in\bigwedge^q(M)$ 成立，其中 q 任意．如果 y 是 0 次齐次元素，则类似的论证成立．所以可以假定 p，$q\geqslant 1$；现在用双重归纳法证明该定理．

745

基础步：$p=1$ 和 $q=1$．假设 $x,y\in\bigwedge^1(M)=M$．现在

$$\begin{aligned}0&=(x+y)\wedge(x+y)\\&=x\wedge x+x\wedge y+y\wedge x+y\wedge y\\&=x\wedge y+y\wedge x.\end{aligned}$$

由此，正如所要的 $x\wedge y=-y\wedge x$．

归纳步：$(p,1)\Rightarrow(p+1,1)$．归纳假设给出

$$(x_1\wedge\cdots\wedge x_p)\wedge y=(-1)^p y\wedge(x_1\wedge\cdots\wedge x_p).$$

用结合性，有

$$\begin{aligned}(x_1\wedge\cdots\wedge x_{p+1})\wedge y&=x_1\wedge[(x_2\wedge\cdots\wedge x_{p+1})\wedge y]\\&=x_1\wedge(-1)^p[y\wedge(x_2\wedge\cdots\wedge x_{p+1})]\\&=[x_1\wedge(-1)^p y]\wedge(x_2\wedge\cdots\wedge x_{p+1})\\&=(-1)^{p+1}(y\wedge x_1)\wedge(x_2\wedge\cdots\wedge x_{p+1}).\end{aligned}$$

归纳步：$(p,q)\Rightarrow(p,q+1)$．假定

$$\begin{aligned}&(x_1\wedge\cdots\wedge x_p)\wedge(y_1\wedge\cdots\wedge y_q)\\&=(-1)^{pq}(y_1\wedge\cdots\wedge y_q)\wedge(x_1\wedge\cdots\wedge x_p).\end{aligned}$$

我们让读者用结合性证明

$$\begin{aligned}&(x_1\wedge\cdots\wedge x_p)\wedge(y_1\wedge\cdots\wedge y_{q+1})\\&=(-1)^{p(q+1)}(y_1\wedge\cdots\wedge y_{q+1})\wedge(x_1\wedge\cdots\wedge x_p).\end{aligned}$$

■

定义 设 n 是正整数并设 $1\leqslant p\leqslant n$．一个递增 $p\leqslant n$-表是指表

$$H=i_1,\cdots,i_p,$$

其中 $1\leqslant i_1<i_2<\cdots<i_p\leqslant n$.

如果 $H=i_1,\cdots,i_p$ 是一个递增 $p\leqslant n$-表，我们记

$$e_H=e_{i_1}\wedge e_{i_2}\wedge\cdots\wedge e_{i_p}.$$

当然，递增 $p\leqslant n$-表的个数和 n 个元素的集合的 p-子集的个数一样，就是$\binom{n}{p}$.

命题9.137 设 M 是有限生成的，比如 $M=\langle e_1,\cdots,e_n\rangle$. 如果 $p\geqslant 1$，则$\bigwedge^p(M)$ 由一切形如 e_H 的元素生成，其中 $H=i_1,\cdots,i_p$ 是递增 $p\leqslant n$-表．

746

证明 M 的每个元素有形如$\sum a_ie_i$ 的表达式，其中 $a_i\in k$. 对 $p\geqslant 1$ 用归纳法证明．设 $m_1\wedge\cdots\wedge m_{p+1}$ 是 $\wedge^{p+1}(M)$ 的一个典型的生成元．根据归纳假设，

$$m_1\wedge\cdots\wedge m_p=\sum_H a_He_H,$$

其中 $a_H\in k$ 且 H 是一个递增 $p\leqslant n$-表．如果 $m_{p+1}=\sum b_je_j$，则

$$m_1\wedge\cdots\wedge m_{p+1}=\Big(\sum_H a_He_H\Big)\wedge\Big(\sum_j b_je_j\Big).$$

每个 $e_j \in \sum b_j e_j$ 通过从右到左地（反）交换可以在 $e_H = e_{i_1} \wedge \cdots \wedge e_{i_p}$ 中移动到任意位置（可能要变号）。当然，如果对某个ℓ有$e_j = e_{i_\ell}$，则该项是 0，从而可以假定在残存楔积中的一切因子都是不同的，并且可以按指标排列成升序．■

系 9.138 如果 M 可以由 n 个元素生成，则对一切 $p > n$，$\bigwedge^p(M) = \{0\}$．

证明 p 个因子的任一楔积必是 0，因为其中必有一个生成元要重复．■

定义 如果 V 是秩为 n 的自由 k-模，则 V 上的一个**格拉斯曼代数**是有幺元（记为 e_0）的 k-代数 $G(V)$ 满足

(a) $G(V)$ 包含 $\langle e_0 \rangle \oplus V$ 作为子模，其中 $\langle e_0 \rangle \cong k$；

(b) $G(V)$ 作为 k-代数由 $\langle e_0 \rangle \oplus V$ 生成；

(c) 对一切 $v \in V, v^2 = 0$；

(d) $G(V)$ 是秩为 2^n 的自由 k-模．

741 页上的计算表明条件"对一切 $v \in V$ 有 $v^2 = 0$"蕴涵"对一切 $u, v \in V$ 有 $vu = -uv$"．$G(V)$ 的候选者是$\bigwedge(V)$，但现阶段尚不清楚如何证明$\bigwedge(V)$ 是自由的以及具有要求的秩．

格拉斯曼代数带来复数共轭的一个推广，这个事实是证明它们的存在性的关键．如果 A 是 k-代数，则一个**代数自同构**是 A 和它自己的 k-代数同构．

定理 9.139 设 V 是以 $e_1, \cdots, e_n$ 为基的自由 k-模，其中 $n \geq 1$．

（i）存在格拉斯曼代数 $G(V)$具有称为**共轭**的代数自同构 $u \mapsto \bar{u}$，满足

$$\bar{\bar{u}} = u;$$

$$\overline{e_0} = e_0;$$

$$\bar{v} = -v \quad 对一切 v \in V.$$

747

（ii）格拉斯曼代数 $G(V)$ 是分次 k-代数

$$G(V) = \sum_p G^p(V).$$

其中

$$G^p(V) = \langle e_H：其中 H 是递增 p-表\rangle$$

[我们已经把$\bigwedge^p(V)$ 中的记号 $e_H = e_{i_1} \wedge \cdots \wedge e_{i_p}$ 推广到 $G^p(V)$ 中的 $e_H = e_{i_1} \cdots e_{i_p}$]．此外，$G^p(V)$ 是自由 k-模，且

$$\operatorname{rank}(G^p(V)) = \binom{n}{p}.$$

证明 （i）对 $n \geq 1$ 用归纳法证明．基础步是显然的：如果 $V = \langle e_1 \rangle \cong k$，令 $G(V) = \langle e_0 \rangle \oplus \langle e_1 \rangle$；注意 $G(V)$ 是秩为 2 的自由 k-模．定义 $G(V)$上的乘法为

$$e_0 e_0 = e_0; \quad e_0 e_1 = e_1 = e_1 e_0; \quad e_1 e_1 = 0.$$

容易验证 $G(V)$ 是 k-代数满足格拉斯曼代数的公理．自同构的定义没有别的选择；必有

$$\overline{ae_0 + be_1} = ae_0 - be_1.$$

最后，易知 $u \mapsto \bar{u}$ 是我们要找的自同构．

关于归纳步，设 V 是秩为 $n+1$ 的自由 k-模，并设 $e_1, \cdots, e_{n+1}$ 是 V 的基．如果 $W = \langle e_1, \cdots, e_n \rangle$，则归纳假设提供格拉斯曼代数 $G(W)$，它是自由的，秩为 2^n，并且对一切 $u \in G(W)$，提供自同构

$u \mapsto \overline{u}$．定义 $G(V)=G(W)\oplus G(W)$，从而 $G(V)$ 是秩为 $2^n+2^n=2^{n+1}$ 的自由模．我们定义

$$(x_1,x_2)(y_1,y_2)=(x_1y_1,x_2\overline{y_1}+x_1y_2)$$

使 $G(V)$ 成为一个 k-代数．

现在验证格拉斯曼代数定义中的四个部分．

(a) 此时，V 不是 $G(V)$ 的子模．每个 $v\in V$ 有形如 $v=w+ae_{n+1}$ 的唯一表达式，其中 $w\in W$ 和 $a\in k$．由

$$v=w+ae_{n+1}\mapsto(w,ae_0)$$

给出的 k-映射 $V\to G(V)$ 是 k-模的同构，我们把 V 和它在 $G(V)$ 中的象等同起来．特别地，e_{n+1} 等同于 $(0,e_0)$．注意，$G(w)$ 中的幺元 $e_0\in G(W)$ 等同于 $G(V)$ 中的 $(e_0,0)$，且 $G(V)$ 中乘法的定义表明 $(e_0,0)$ 是 $G(V)$ 中的幺元．

(b) 根据归纳假设，我们知道 $\langle e_0\rangle\oplus W$ 的元素生成作为 k-代数的 $G(W)$，即一切 $(x_1,0)\in G(W)$ 都由 W 的元素形成．其次，由我们的等同看法，$e_{n+1}=(0,e_0)$，

$$(x_1,0)e_{n+1}=(x_1,0)(0,e_0)=(0,x_1),$$

748

从而 V 的元素生成一切形如 $(0,x_2)$ 的对．因加法是坐标状态的，一切 $(x_1,x_2)=(x_1,0)+(0,x_2)$ 由 V 用代数运算形成．

(c) 如果 $v\in V$，则 $v=w+ae_{n+1}$，其中 $w\in W$，且在 $G(V)$ 中，v 等同于 (w,ae_0)．因此，

$$v^2=(w,ae_0)(w,ae_0)=(w^2,ae_0\overline{w}+ae_0w).$$

现在 $w^2=0$，$\overline{w}=-w$，从而 $v^2=0$.

(d) 因为 $G(V)=G(W)\oplus G(W)$，所以 $\mathrm{rank}G(V)=2^{n+1}$.

我们已经证明了 $G(V)$ 是格拉斯曼代数．最后，定义共轭为

$$\overline{(x_1,x_2)}=(\overline{x}_1,-\overline{x}_2).$$

读者可以验证它定义了一个具有所需性质的函数．

(ii) 对 $n\geqslant 1$ 用归纳法证明 $G^p(V)=\langle e_H$：其中 H 是递增 p－表$\rangle$ 是自由 k-模，且以表达式中显示的积 e_H 为基．基础步是显然的：如果 $\mathrm{rank}(V)=1$，比如有基 e_1，则 $G(V)=\langle e_0,e_1\rangle$；此外，$G^0(V)$ 和 $G^1(V)$ 都是自由的，秩都是 1.

关于归纳步，假定 V 是自由的且以 $e_1,\cdots,e_{n+1}$ 为基．和(i)的证明一样，设 $W=\langle e_1,\cdots,e_n\rangle$. 根据归纳假设，$G^p(W)$ 是自由 k-模，秩为 $\binom{n}{p}$，且以一切 e_H 为基，其中 H 是递增 $p\leqslant n$-表．$G^p(V)$ 有两种类型的元素：元素 $e_H\in G(W)$，其中 H 是递增 $p\leqslant n$-表；元素 $e_H=e_{i_1},\cdots e_{i_{p-1}}e_{n+1}$，其中 H 是涉及 e_{n+1} 的递增 $p\leqslant(n+1)$-表．我们知道第一类型的元素组成 $G(W)$ 的基．$G(V)$ 中乘法的定义给出 $e_He_{n+1}=(e_H,0)(0,e_0)=(0,e_H)$．于是这种积的个数是 $\binom{n}{p-1}$. 因 $G(V)=G(W)\oplus G(W)$，我们知道这两种类型的积的并形成 $G^p(V)$ 的基，从而 $\mathrm{rank}(G^p(V))=\binom{n}{p}+\binom{n}{p-1}=\binom{n+1}{p}$.

剩下要证明 $G^p(V)G^q(V)\subseteq G^{p+q}(V)$. 考虑 $e_{i_1}\cdots e_{i_p}e_{j_1}\cdots e_{j_q}$. 如果某个下标 i_r 和下标 j_s 相同，则因这种积中有重复因子，所以等于 0；如果一切下标都不同，则这个积正如所要的是在 $G^{p+q}(V)$

中．所以，$G(V)$ 是分次 k-代数，它的 p 次分次部分是秩为 $\binom{n}{p}$ 的自由 k-模． ■

定理 9.140（二项式定理） 如果 V 是秩为 n 的自由 k-模，则存在分次 k-代数的同构，

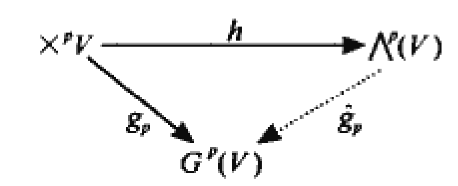
$$\bigwedge(V) \cong G(V).$$

于是，对一切 $p \geqslant 1$，$\bigwedge^p(V)$ 是自由 k-模，且以一切递增 $p \leqslant n$-表为基，因此

$$\operatorname{rank}\left(\bigwedge^p(V)\right) = \binom{n}{p}.$$

749

证明 对任意 $p \geqslant 2$，考虑图



其中 $g_p(v_1, \cdots, v_p) = v_1 \cdots v_p$．因对一切 $v \in V$，在 $G^p(V)$ 中 $v^2 = 0$，所以函数 g_p 是交错多重线性的．根据外幂的泛性，存在（唯一）h-同态 $\hat{g}_p : \bigwedge^p(V) \to G^p(V)$ 使得图交换；即

$$\hat{g}_p(v_1 \wedge \cdots \wedge v_p) = v_1 \cdots v_p.$$

如果 $e_1, \cdots, e_n$ 是 V 的基，则我们刚才已经看到 $G^p(V)$ 是以一切 $e_{i_1} \cdots e_{i_p}$ 为基的自由 k-模，从而 $\hat{g}_p$ 是满射．但根据命题 9.137 $\bigwedge^p(V)$ 由一切 $e_{i_1} \wedge \cdots \wedge e_{i_p}$ 生成．如果某个 k-线性组合 $\sum_H a_H e_H$ 在 $\ker \hat{g}_p$ 中，则在 $G^p(V)$ 中 $\sum_H a_H \hat{g}_p(e_H) = 0$．但象 $\hat{g}_p(e_H)$ 的表形成自由 k-模 $G^p(V)$ 的基，从而一切系数 $a_H = 0$．所以，$\ker \hat{g}_p = \{0\}$，因此 $\hat{g}_p$ 是 k-同构．

定义 $\gamma : \bigwedge(V) \to G(V)$ 为 $\gamma\left(\sum_{p=0}^{n} u_p\right) = \sum_{p=0}^{n} \hat{g}_p(u_p)$，从而 $\gamma(\bigwedge^p(V)) \subseteq G^p(V)$．如果能够证明 γ 是代数映射：$\gamma(u \wedge v) = \gamma(u)\gamma(v)$ 定理就得以证明．但这对 $\bigwedge(V)$ 的齐次元素显然成立，因此对一切元素成立． ■

系 9.141 如果 V 是以 $e_1, \cdots, e_n$ 为基的自由 k-模，则

$$\bigwedge^n(V) = \langle e_1 \wedge \cdots \wedge e_n \rangle \cong k.$$

证明 根据命题 9.137，我们知道 $\bigwedge^n(V)$ 是由 $e_1 \wedge \cdots \wedge e_n$ 生成的循环模，但不能从该命题推出这个元素是否为零．然而，二项式定理不仅说这个元素非零，而且说它生成同构于 k 的循环模． ■

命题 7.43 说，如果 $T : {}_k\mathbf{Mod} \to {}_k\mathbf{Mod}$ 是加性函子，则 $T(V \oplus V') \cong T(V) \oplus T(V')$．由此，对 $p \geqslant 2$，$\bigwedge^p$ 不是加性函子：如果 V 是秩为 n 的自由 k-模，则 $\bigwedge^p(V \oplus V)$ 是秩为 $\binom{2n}{p}$ 的自由 k-模，而 $\bigwedge^p(V) \oplus \bigwedge^p(V)$ 是秩为 $2\binom{n}{p}$ 的自由 k-模．

敏感的读者会注意到我们构造的格拉斯曼代数 $G(V)$ 不仅依赖于自由 k-模 V，也依赖于 V 的基的选取．如果选取 V 的另外一组基，第二个格拉斯曼代数会和第一个同构吗？

系 9.142 设 V 是自由 k-模，并设 B 和 B' 都是 V 的基．如果 $G(V)$ 是用 B 定义的格拉斯曼代数，$G'(V)$ 是用 B' 定义的格拉斯曼代数，则作为分次 k-代数有 $G(V) \cong G'(V)$．

750

证明 $G(V)$和$G'(V)$都同构于$\bigwedge(V)$，而$\bigwedge(V)$ 的定义中没有用到基的选取. ■

下面的结果给出二项式定理的另一个证明.

定理 9.143 对一切 $p\geqslant 0$ 和一切 k-模 A 和 B，其中 k 是交换环.

$$\bigwedge^p(A\oplus B)\cong\sum_{i=0}^{p}(\bigwedge^i(A)\otimes_k\bigwedge^{p-i}(B)).$$

证明概要 设$\mathcal{A}$是一切交错反交换分次 k-代数 $R=\sum_{p\geqslant 0}R^p$（对一切奇次数 $r\in R$ 有 $r^2=0$，且对 $r\in R^p$ 和 $s\in R^q$ 有 $rs=(-1)^{pq}sr$）的范畴；根据定理 9.136，对每个 k-模 A，外代数$\bigwedge(A)\in\operatorname{obj}(\mathcal{A})$. 如果 $R,S\in\operatorname{obj}(\mathcal{A})$，则可以验证 $R\otimes_k S=\sum_{p\geqslant 0}(\sum_{i=0}^{p}R^i\otimes_k S^{p-i})\in\operatorname{obj}(\mathcal{A})$；用反交换性，对命题 9.101 作适度的推广可以证明$\mathcal{A}$有余积.

我们断言 $(\bigwedge,D)$ 是函子的伴随对，其中$\bigwedge:{}_k\mathbf{Mod}\to\mathcal{A}$ 发送 $A\mapsto\bigwedge(A)$，$D:\mathcal{A}\to{}_k\mathbf{Mod}$ 发送 $\sum_{p\geqslant 0}R^p\mapsto R^1$，$R^1$ 是次数为 1 的项. 如果 $R=\sum_p R^p$，则存在映射 $\pi_R:\bigwedge(R^1)\to R$；定义 $\tau_{A,R}:\operatorname{Hom}_{\mathcal{A}}(\bigwedge(A),R)\to\operatorname{Hom}_k(A,R^1)$ 为 $\varphi\mapsto\pi_R(\varphi\mid A)$，由定理 7.105，$\bigwedge$保持余积；即$\bigwedge(A\oplus B)\cong\bigwedge(A)\otimes_k\bigwedge(B)$，从而$\bigwedge^p(A\oplus B)\cong\sum_{i=0}^{p}(\bigwedge^i(A)\otimes_k\bigwedge^{p-i}(B))$. ■

下面是一个同构的显式公式. 在 $\bigwedge^3(A\oplus B)$ 中，有

$$\begin{aligned}(a_1+b_1)\wedge(a_2+b_2)\wedge(a_3+b_3)=&\ a_1\wedge a_2\wedge a_3+a_1\wedge b_2\wedge a_3\\&+b_1\wedge a_2\wedge a_3+b_1\wedge b_2\wedge a_3+a_1\wedge a_2\wedge b_3\\&+a_1\wedge b_2\wedge b_3+b_1\wedge a_2\wedge b_3+b_1\wedge b_2\wedge b_3.\end{aligned}$$

由反交换性，可以把每个 a 写在一切 b 的前面：

$$\begin{aligned}(a_1+b_1)\wedge(a_2+b_2)\wedge(a_3+b_3)=&\ a_1\wedge a_2\wedge a_3-a_1\wedge a_3\wedge b_2\\&+a_2\wedge a_3\wedge b_1+a_3\wedge b_1\wedge b_2+a_1\wedge a_2\wedge b_3\\&+a_1\wedge b_2\wedge b_3-a_2\wedge b_1\wedge b_3+b_1\wedge b_2\wedge b_3.\end{aligned}$$

一个 i-洗牌是指把 $\{1,2,\cdots,p\}$ 分成不相交的两个子集 $\mu_1<\cdots<\mu_i$ 和 $v_1<\cdots<v_{p-i}$ 的一个划分；它给出置换 $\sigma\in S_p$ 使得对 $j\leqslant i,\sigma(j)=\mu_j$ 和对 $j=i+\ell>i,\sigma(i+\ell)=v_\ell$. $(a_1+b_1)\wedge(a_2+b_2)\wedge(a_3+b_3)$ 中的每个"混合"项给出一个洗牌，其中 a 给出 μ，b 给出 v；例如，$a_1\wedge b_2\wedge a_3$ 是一个 2-洗牌，$b_1\wedge a_2\wedge b_3$ 是一个 1-洗牌. 现在 $\operatorname{sgn}(\sigma)$ 把左移各个 a 到一切 b 前面的总次数计算在内，读者可以验证在重写后的表达式中的符号是 $\operatorname{sgn}(\sigma)$. 定义 $f:\bigwedge^p(A\oplus B)\to\sum_{i=0}^{p}(\bigwedge^i(A)\otimes_k\bigwedge^{p-i}(B))$ 为

$$f(a_1+b_1,\cdots,a_p+b_p)=\sum_{i=0}^{p}\Big[\sum_{i\text{-洗牌}\sigma}\operatorname{sgn}(\sigma)a_{\mu_1}\wedge\cdots\wedge a_{\mu_i}\otimes b_{v_1}\wedge\cdots\wedge b_{v_{p-i}}\Big].$$

751

系 9.144 如果 k 是交换环和 V 是秩为 n 的自由 k-模，则 $\bigwedge^p(V)$ 是秩为 $\binom{n}{p}$ 的自由 k-模.

证明 写 $V=k\oplus B$ 并对 $\operatorname{rank}(V)$ 用归纳法即可. ■

在下一节中将用外代数证明关于行列式的定理，但要先注意当 k 是域时的一个很好的结果，此时 k-模是向量空间.

命题 9.145 设 k 是域，V 是 k 上的向量空间，并设 $v_1,\cdots,v_p$ 是 V 中的向量．则在$\bigwedge(V)$中 $v_1\wedge\cdots\wedge v_p=0$ 当且仅当 $v_1,\cdots,v_p$ 是线性相关表．

证明 因 k 是域，一个线性无关表 $v_1,\cdots,v_p$ 可以扩展为 V 的一组基 $v_1,\cdots,v_p,\cdots,v_n$，根据系 9.141，$v_1\wedge\cdots\wedge v_n\neq 0$．但 $v_1\wedge\cdots\wedge v_p$ 是 $v_1\wedge\cdots\wedge v_n$ 的因子，因此 $v_1\wedge\cdots\wedge v_p\neq 0$．

反之，如果 $v_1,\cdots,v_p$ 线性相关，则存在某个 i 使得 $v_i=\sum_{j\neq i}a_jv_j$，其中 $a_j\in k$．因此

$$\begin{aligned}v_1\wedge\cdots\wedge v_i\wedge\cdots\wedge v_p &= v_1\wedge\cdots\wedge\sum_{j\neq i}a_jv_j\wedge\cdots\wedge v_p\\ &= \sum_{j\neq i}a_jv_1\wedge\cdots\wedge v_j\wedge\cdots\wedge v_p.\end{aligned}$$

展开后每一项都有重复因子 v_j，因此是 0. ■

本节开始时，我们基于对雅可比行列式的观察引入外代数；现在则把外代数运用到微分形式上以结束本节．设 X 是欧几里得空间$\mathbb{R}^n$ 的连通[⊖]开子集．如果函数 $f: X\to\mathbb{R}$ 对一切 $p\geqslant 1$ 和 $i=1,\cdots,n$ 存在 p 次偏导数$\partial^p f/\partial^p x_i$ 和一切混合偏导数，则称 f 为 C^∞-函数．

定义 如果 X 是$\mathbb{R}^n$ 的连通开子集，定义

$$A(X)=\{f: X\to\mathbb{R}: f\text{ 是 }C^\infty\text{-函数}\}.$$

因为有 X 是$\mathbb{R}^n$ 的连通开子集的条件，所以 C^∞-函数有定义．易知 $A(X)$在点态运算下是交换环：

$$f+g: x\mapsto f(x)+g(x);\ fg: x\mapsto f(x)g(x).$$

在一切 n 元组的自由 $A(X)$-模 $A(X)^n$ 中，重新命名标准基

752

$$dx_1,\cdots,dx_n.$$

根据二项式定理，每个元素 $\omega\in\bigwedge^p(A(X)^n)$ 有唯一表达式

$$\omega=\sum_{i_1\cdots i_p}f_{i_1\cdots i_p}dx_{i_1}\wedge\cdots\wedge dx_{i_p},$$

其中 $f_{i_1\cdots i_p}\in A(X)$是 X 上的 C^∞-函数且 $i_1\cdots i_p$ 是递增 $p\leqslant n$-表．我们记

$$\Omega^p(X)=\bigwedge^p(A(X)^n),$$

并把它的元素称为 X 上的 p **阶微分形式**．

定义 **外导数** $d^p:\Omega^p(X)\to\Omega^{p+1}(X)$定义如下：

（ⅰ）如果 $f\in\Omega^0(X)=A(X)$，则 $d^0f=\sum_{j=1}^{n}\frac{\partial f}{\partial x_j}dx_j$；

（ⅱ）如果 $p\geqslant 1$ 且 $\omega\in\Omega^p(X)$，则 $\omega=\sum_{i_1\cdots i_p}f_{i_1\cdots i_p}dx_{i_1}\wedge\cdots\wedge dx_{i_p}$，定义

$$d^p\omega=\sum_{i_1\cdots i_p}d^0(f_{i_1\cdots i_p})\wedge dx_{i_1}\wedge\cdots\wedge dx_{i_p}.$$

如果 X 是$\mathbb{R}^n$ 的连通开子集，外导数给出 $A(X)$－映射的序列，叫做**德拉姆复形**：

$$0\to\Omega^0(X)\xrightarrow{d^0}\Omega^1(X)\xrightarrow{d^1}\cdots\xrightarrow{d^{n-1}}\Omega^n(X)\to 0.$$

命题 9.146 如果 X 是$\mathbb{R}^n$ 的连通开子集，则

$$d^{p+1}d^p:\Omega^p(X)\to\Omega^{p+2}(X)$$

⊖ 如果 X 是子集，对每个 $x\in X$，存在某个 $r>0$，使得距离 $|y-x|<r$ 的一切点 y 都在 X 中，则称 X 为开集．如果 X 是$\mathbb{R}^n$ 中的开子集，且 X 中的任意两点都有一条整个都在 X 中的路径把它们连接起来，则称 X 是连通的．

对一切 $p\geqslant 0$ 是零映射．

证明 只要证明 $\mathrm{dd}\omega=0$，其中 $\omega=f\mathrm{d}x_I$（用早先的缩写记号：$\mathrm{d}x_I=\mathrm{d}x_{i_1}\wedge\cdots\wedge\mathrm{d}x_{i_p}$，其中 $I=i_1,\cdots,i_p$ 是递增 $p\leqslant n$-表）．

现在

$$\begin{aligned}\mathrm{dd}\omega&=\mathrm{d}(\mathrm{d}^0 f\wedge x_I)\\&=\mathrm{d}\Big(\sum_i\frac{\partial f}{\partial x_i}\mathrm{d}x_i\wedge\mathrm{d}x_I\Big)\\&=\sum_i\sum_j\frac{\partial^2 f}{\partial x_i\,\partial x_j}\mathrm{d}x_j\wedge\mathrm{d}x_i\wedge\mathrm{d}x_I.\end{aligned}$$

在这个双重和式中，比较 i，j 和 j，i 项：第一个是

$$\frac{\partial^2 f}{\partial x_i\,\partial x_j}\mathrm{d}x_j\wedge\mathrm{d}x_i\wedge\mathrm{d}x_I;$$

753

第二个是

$$\frac{\partial^2 f}{\partial x_j\,\partial x_i}\mathrm{d}x_i\wedge\mathrm{d}x_j\wedge\mathrm{d}x_I.$$

它们互相抵消，这是因为二阶混合偏导数相等：

$$\mathrm{d}x_i\wedge\mathrm{d}x_j=-\mathrm{d}x_j\wedge\mathrm{d}x_i.$$

■

例 9.147 考虑 $n=3$ 的德拉姆复形的特殊情形．

$$0\to\Omega^0(X)\xrightarrow{\mathrm{d}^0}\Omega^1(X)\xrightarrow{\mathrm{d}^1}\Omega^2(X)\xrightarrow{\mathrm{d}^2}\Omega^3(X)\to 0$$

如果 $\omega\in\Omega^0(X)$，则 $\omega=f(x,y,z)\in A(X)$，且

$$\mathrm{d}^0 f=\frac{\partial f}{\partial x}\mathrm{d}x+\frac{\partial f}{\partial y}\mathrm{d}y+\frac{\partial f}{\partial z}\mathrm{d}z,$$

它是类似 $\mathrm{grad}(f)$ 的 1 阶形式．

如果 $\omega\in\Omega^1(X)$，则 $\omega=f\mathrm{d}x+g\mathrm{d}y+h\mathrm{d}z$，经简单计算得

$$\mathrm{d}^1\omega=\Big(\frac{\partial g}{\partial x}-\frac{\partial f}{\partial y}\Big)\mathrm{d}x\wedge\mathrm{d}y+\Big(\frac{\partial h}{\partial y}-\frac{\partial g}{\partial z}\Big)\mathrm{d}y\wedge\mathrm{d}z+\Big(\frac{\partial f}{\partial z}-\frac{\partial h}{\partial x}\Big)\mathrm{d}z\wedge\mathrm{d}x,$$

它是类似 $\mathrm{curl}(\omega)$ 的 2 阶形式．

如果 $\omega\in\Omega^2(X)$，则 $\omega=F\mathrm{d}y\wedge\mathrm{d}z+G\mathrm{d}z\wedge\mathrm{d}x+H\mathrm{d}x\wedge\mathrm{d}y$．现在

$$\mathrm{d}^2\omega=\frac{\partial F}{\partial x}+\frac{\partial G}{\partial y}+\frac{\partial H}{\partial z},$$

它是类似 $\mathrm{div}(\omega)$ 的 3 阶形式．

它们不仅仅是类似的．因 $\Omega^1(X)$ 是以 $\mathrm{d}x,\mathrm{d}y,\mathrm{d}z$ 为基的自由 $A(X)$-模，我们知道当 ω 是 0 阶形式时，$\mathrm{d}^0(\omega)$是 $\mathrm{grad}(\omega)$．现在 $\Omega^2(X)$ 是自由 $A(X)$-模，选取基

$$\mathrm{d}x\wedge\mathrm{d}y,\mathrm{d}y\wedge\mathrm{d}z,\mathrm{d}z\wedge\mathrm{d}x$$

而不是通常的基 $\mathrm{d}x\wedge\mathrm{d}y,\mathrm{d}x\wedge\mathrm{d}z,\mathrm{d}y\wedge\mathrm{d}z$；从而此时 $\mathrm{d}^1(\omega)$ 是 $\mathrm{curl}(\omega)$．最后，$\Omega^3(X)$ 以 $\mathrm{d}x\wedge\mathrm{d}y\wedge\mathrm{d}z$ 为基，因此，当 ω 是 2 阶形式时，$\mathrm{d}^3(\omega)$ 是 $\mathrm{div}(\omega)$．我们已经证明德拉姆复形是

$$0\to\Omega^0(X)\xrightarrow{\mathrm{grad}}\Omega^1(X)\xrightarrow{\mathrm{curl}}\Omega^2(X)\xrightarrow{\mathrm{div}}\Omega^3(X)\to 0.$$

现在命题 9.146 给出高等微积分中熟知的恒等式：

$$\mathrm{curl}\cdot\mathrm{grad}=0\text{ 和 }\mathrm{div}\cdot\mathrm{curl}=0.$$

754

如果 $d\omega=0$，则称 1 阶形式 ω 是闭的，如果有某个 C^∞-函数 f 使得 $\omega=\operatorname{grad} f$，则称 ω 是正合的．一般地，如果 $d^p\omega=0$，则称 p 阶形式 ω 是闭的，而如果有某个 $(p-1)$-形式 ω' 使得 $\omega=d^{p-1}\omega'$，则称 ω 是正合的．于是，$\omega\in\Omega^p(X)$ 是闭的当且仅当 $\omega\in\ker d^p$，而 ω 是正合的当且仅当 $\omega\in\operatorname{im} d^{p-1}$．所以，德拉姆复形是 $A(X)$-模的正合列当且仅当每个闭形式都是正合的；这就是在"正合列"中正合这个形容词的语义．可以证明，只要 X 是$\mathbb{R}^n$ 的单连通开子集，则德拉姆复形是正合列．对任意（不必单连通）空间 X，我们有 $\operatorname{im}\operatorname{grad}\subseteq\ker\operatorname{curl}$ 和 $\operatorname{im}\operatorname{curl}\subseteq\ker\operatorname{div}$，$\mathbb{R}$-向量空间 $\ker\operatorname{curl}/\operatorname{im}\operatorname{grad}$ 和 $\ker\operatorname{div}/\operatorname{im}\operatorname{curl}$ 称为 X 上的上同调群． ■

习题

9.85 设 $G(V)$ 是自由 k-模 V 的格拉斯曼代数，并设 $u=\sum_p u_p\in G(V)$，其中 $u_p\in G^p(V)$ 是 p 次齐次元素．如果 $\bar{u}$ 是定理 9.139 中的 u 的共轭，证明 $\bar{u}=\sum_p(-1)^p u_p$．

9.86 (i) 设 p 是素数．证明$\bigwedge^2(\mathbb{I}_p\oplus\mathbb{I}_p)\neq 0$，其中$\mathbb{I}_p\oplus\mathbb{I}_p$ 看作$\mathbb{Z}$-模（即看作阿贝尔群）．

(ii) 设 $D=\mathbb{Q}/\mathbb{Z}\oplus\mathbb{Q}/\mathbb{Z}$．证明 $\bigwedge^2(D)=0$，并由此推出如果 $i:\mathbb{I}_p\oplus\mathbb{I}_p\to D$ 是包含映射，则$\bigwedge^2(i)$ 不是单射．

9.87 (i) 如果 k 是交换环和 N 是一个 k-模 M 的直和项，证明对一切 $p\geqslant 0$，$\bigwedge^p(N)$ 是 $\bigwedge^p(M)$ 的直和项．

提示：用系 7.17.

(ii) 如果 k 是域和 $i:W\to V$ 是 k 上向量空间的单射，证明对一切 $p\geqslant 0$，$\bigwedge^p(i)$ 是单射．

9.88 证明对一切 p，函子$\bigwedge^p$保持满射．

9.89 如果 P 是投射 k-模，其中 k 是交换环．证明对一切 q，$\bigwedge^q(P)$ 是投射 k-模．

9.90 设 k 是域并设 V 是 k 上的向量空间．证明两个线性无关表 $u_1,\cdots,u_p$ 和 $v_1,\cdots,v_p$ 张成 V 的同一子空间当且仅当存在非零 $c\in k$ 使得 $u_1\wedge\cdots\wedge u_p=cv_1\wedge\cdots\wedge v_p$．

9.91 如果 U 和 V 都是交换环 R 上的 R-模，且 $U'\subseteq U$，$V'\subseteq V$ 是子模，证明

$$(U\otimes_R V)/(U'\otimes_R V+U\otimes_R V')\cong(U/U')\otimes(V/V').$$

提示：定义 $\varphi:U\otimes_R V\to(U/U')\otimes(V/V')$ 为 $\varphi:u\otimes v\mapsto(u+U')\otimes v+u\otimes(v+V')$，计算 φ 的核和象．

9.92 定义 k-模 M 上的**对称代数**为 $S(M)=T(M)/I$，其中 I 是由一切 $m\otimes m'-m'\otimes m$ 生成的双边理想，其中 $m,m'\in M$.

(i) 证明 I 是分次理想，从而 $S(M)$ 是分次 k-代数．

755

(ii) 证明 $S(M)$ 是交换的．

9.93 (i) 定义**自由交换 k-代数**，并证明如果 M 是以 X 为基的自由 k-模，则 $S(M)$ 是 X 上的自由交换 k-代数．由此推出 $S(M)$ 不依赖于自由 k-模 M 的基的选取．

(ii) 定义 $k[X]$ 为变量 X 交换的多项式环，如果每个 $u\in K[X]$ 有唯一的多项式表达式，该多项式的变量是 X 中的有限个元素．证明：如果 M 是以 X 为基的自由 k-模，则 $S(M)$是变量 X 交换的多项

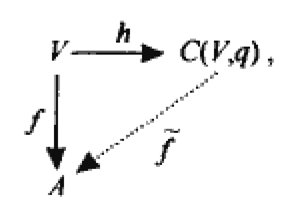
式环[⊖].

（iii）证明：如果 M 是有有限秩 n 的自由 k-模，则 $S^p(M)$是秩为$\binom{n+p-1}{p}$的自由 k-模.

提示：用组合事实：把 p 个相同的对象放到 n 个盒中共有$\binom{n+p-1}{p}$种放法.

（iv）证明每个交换 k-代数都是一个自由交换 k-代数的商.

9.94 设 V 是域 k 上的有限维向量空间，并设 $q: V \to k$ 是 V 上的二次型．定义**克利福德代数** $C(V,q)$ 为商 $C(V,q) = T(V)/J$，其中 J 是由形如 $v \otimes v - q(v)1$ 的一切元素生成的双边理想（注意 J 不是分次理想）．对 $v \in V$，记陪集 $v+J$ 为 $[v]$，并定义 $h: V \to C(V,q)$ 为 $h(v) = [v]$. 证明 $C(V,q)$ 是下面泛问题的解：



其中 A 是 k-代数，$f: V \to A$ 是满足对一切 $v \in V$ 有 $f(v)^2 = q(v)$ 的 k-模映射．

如果 $\dim(V) = n$ 且 q 非退化，则可以证明 $\dim(C(V,q)) = 2^n$. 特别地，如果 $k = \mathbb{R}$ 和 $n = 2$，则克利福德代数的维数是 4，且 $C(v,q) \cong \mathbb{H}$，$\mathbb{H}$ 是四元数除环．克利福德代数用来研究二次型，因此也用来研究正交群；见 Jacobson 所著的《Basic Algebra II》，228～245 页．

9.9 行列式

我们已经使用了行列式的熟知性质，虽然读者可能看到这些性质只在域上而不是在一般的交换环上得到验证．因元素在交换环中的矩阵的行列式很重要，所以现在就在一般情形下建立这些性质，因为现在可以用外代数帮助我们．

如果 k 是交换环，我们断言每个 k-模映射 $\gamma: k \to k$ 恰是乘以某个 $d \in k$：如果 $\gamma(1) = d$，则对一切 $a \in k$，因为 γ 是 k-模映射，所以有

$$\gamma(a) = \gamma(a1) = a\gamma(1) = ad = da.$$

756

这里稍作推广．如果 $V = \langle v \rangle \cong k$，则每个 k-映射 $\gamma: V \to V$ 有 $\gamma: av \mapsto dav$ 的形式，其中 $\gamma(v) = dv$. 现在假定 V 是以 $e_1, \cdots, e_n$ 为基的自由 k-模；系 9.141 表明$\bigwedge^n(V)$ 是自由的，秩为 1，生成元是 $e_1 \wedge \cdots \wedge e_n$. 由此，每个 k-映射 $\gamma: \bigwedge^n(V) \to \bigwedge^n(V)$ 形如 $\gamma(a(e_1 \wedge \cdots \wedge e_n)) = d(a(e_1 \wedge \cdots \wedge e_n))$.

定义 如果 V 是以 $e_1, \cdots, e_n$ 为基的自由 k-模，$f: V \to V$ 是 k-同态，则 f 的**行列式**（记为 $\det(f)$）是指元素 $\det(f) \in k$ 满足

$$\begin{aligned}\textstyle\bigwedge^n(f): e_1 \wedge \cdots \wedge e_n &\mapsto f(e_1) \wedge \cdots \wedge f(e_n) \\ &= \det(f)(e_1 \wedge \cdots \wedge e_n).\end{aligned}$$

如果 $A = [a_{ij}]$ 是元素在 k 中的 $n \times n$ 矩阵，则 A 由 $f(x) = Ax$ 定义了一个 k-映射 $f: k^n \to k^n$，其中 $x \in k^n$ 是列向量．如果 $e_1, \cdots, e_n$ 是 k^n 的标准基，则 $f(e_i) = \sum_j a_{ji} e_j$，且与 f 相伴的矩阵 $A =$

⊖ 在第 6.4 节中，为了构造一个域的代数闭包，我们假定这个大多项式环存在．
我们早先定义 $k[x,y]$为 $R[y]$，其中 $R=k[x]$，这是很粗心的．例如，不能得到 $k[x,y]=k[y,x]$，虽然这两个环是同构的．然而，如果 M 是以 x，y 为基的自由 k-模，则 y，x 也是 k-代数 M 的基，从而 $k[x,y]=k[y,x]$.

$[a_{ij}]$ 的第 i 列是 $f(e_i)=Ae_i$ 的坐标．我们定义 $\det(A)=\det(f)$：

$$Ae_1\wedge\cdots\wedge Ae_n=\det(A)(e_1\wedge\cdots\wedge e_n).$$

于是，A 的列在 $\bigwedge^n(k^n)$ 中的楔积是 $e_1\wedge\cdots\wedge e_n$ 乘以常数，而这个常数就是 $\det(A)$.

例 9.148 如果

$$A=\begin{bmatrix}a & c\\ b & d\end{bmatrix},$$

则 A 的列的楔积是

$$\begin{aligned}(ae_1+be_2)\wedge(ce_1+de_2)&=ace_1\wedge e_1+ade_1\wedge e_2+bce_2\wedge e_1+bde_2\wedge e_2\\&=ade_1\wedge e_2+bce_2\wedge e_1\\&=ade_1\wedge e_2-bce_1\wedge e_2\\&=(ad-bc)(e_1\wedge e_2).\end{aligned}$$

所以，$\det(A)=ad-bc$. ■

读者或许注意到这个计算是 742 页上的计算的重复，那里我们计算了二重积分中变量替换的雅可比行列式．下一例考虑三重积分．

例 9.149 在三重积分 $\iiint_D f(x,y,z)\mathrm{d}x\mathrm{d}y\mathrm{d}z$ 中用等式：

$$x=F(u,v,w);$$
$$y=G(u,v,w);$$
$$z=H(u,v,w)$$

757

作变量替换．记 $f(x,y,z)$ 在点 $P=(x_0,y_0,z_0)$ 处切空间 T 的基为 $\mathrm{d}x,\mathrm{d}y,\mathrm{d}z$．如果 $\mathrm{d}u,\mathrm{d}v,\mathrm{d}w$ 是 T 的另一组基，则链式法则由等式

$$\mathrm{d}x=F_u\mathrm{d}u+F_v\mathrm{d}v+F_w\mathrm{d}w$$
$$\mathrm{d}y=G_u\mathrm{d}u+G_v\mathrm{d}v+G_w\mathrm{d}w$$
$$\mathrm{d}z=H_u\mathrm{d}u+H_v\mathrm{d}v+H_w\mathrm{d}w$$

定义了 T 上的线性变换．如果在被积函数中把微分 $\mathrm{d}x\mathrm{d}y\mathrm{d}z$ 写作 $\mathrm{d}x\wedge\mathrm{d}y\wedge\mathrm{d}z$，则变量替换给出新的微分

$$\mathrm{d}x\wedge\mathrm{d}y\wedge\mathrm{d}z=\det\left(\begin{bmatrix}F_u & F_v & F_w\\ G_u & G_v & G_w\\ H_u & H_v & H_w.\end{bmatrix}\right)\mathrm{d}u\wedge\mathrm{d}v\wedge\mathrm{d}w.$$

展开

$$(F_u\mathrm{d}u+F_v\mathrm{d}v+F_w\mathrm{d}w)\wedge(G_u\mathrm{d}u+G_v\mathrm{d}v+G_w\mathrm{d}w)\wedge(H_u\mathrm{d}u+H_v\mathrm{d}v+H_w\mathrm{d}w)$$

得到 9 项，其中 3 项涉及 $(\mathrm{d}u)^2,(\mathrm{d}v)^2$ 或 $(\mathrm{d}w)^2$，因而为 0. 剩下的 6 个之中，有 3 个带负号，易知这个和就是行列式． ■

命题 9.150 *设 k 是交换环．*

（i）*如果 I 是单位矩阵，则 $\det(I)=1$.*

（ii）*如果 A 和 B 都是元素在 k 中的 $n\times n$ 矩阵，则*

$$\det(AB)=\det(A)\det(B).$$

证明 两个结果都由 $\bigwedge^n$ 中是 ${}_k\mathbf{Mod}$ 中的函子得到．

（ⅰ）对应于单位矩阵的线性变换是 1_{k^n}，每个函子把单位变到单位．

（ⅱ）如果 f 和 g 分别是由矩阵 A 和 B 形成的 k^n 上的线性变换，则 fg 是由 AB 形成的线性变换．如果记 $e_1\wedge\cdots\wedge e_n$ 为 e_N，则

$$\begin{aligned}\det(fg)e_N &= \bigwedge^n(fg)(e_N)\\ &= \bigwedge^n(f)\left(\bigwedge^n(g)(e_N)\right)\\ &= \bigwedge^n(f)\det(g)e_N)\\ &= \det(g)\bigwedge^n(f)(e_N)\\ &= \det(f)\det(g)e_N;\end{aligned}$$

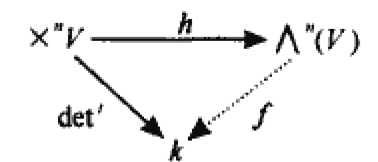
758

倒数第二步的推出用到了 $\bigwedge^n(f)$ 是 k-映射的事实．所以

$$\det(AB)=\det(fg)=\det(f)\det(g)=\det(A)\det(B).$$ ■

系 9.151 *如果 k 是交换环，则 $\det:\mathrm{Mat}_n(k)\to k$ 是唯一的交错多重线性函数使得 $\det(I)=1$.*

证明 行列式的定义（作为列的楔积）表明它是交错多重线性函数 $\det:\times^n V\to k$，其中 $V=k^n$，上面的命题表明 $\det(I)=1$. 这种函数的唯一性来自 $\bigwedge^n$的泛性．



如果 det′是多重线性的，则存在 k-映射 $f:\bigwedge^n(V)\to k$ 使得 $fh=\det'$；如果 $\det'(e_1,\cdots,e_n)=1$，则 $f(e_1\wedge\cdots\wedge e_n)=1$．因$\bigwedge^n(V)\cong k$，每个 k-映射 $f:\bigwedge^n(V)\to k$ 由 $f(e_1\wedge\cdots\wedge e_n)$ 确定．于是，映射 f 关于 det′和关于 det 是一样的，从而 $\det'=fh=\det$． ■

现在证明刚才定义的行列式和我们熟知的行列式函数一致．

引理 9.152 *设 $e_1,\cdots,e_n$ 是自由 k-模的基，其中 k 是交换环．如果 σ 是 1，2，…，n 的置换，则*

$$e_{\sigma(1)}\wedge\cdots\wedge e_{\sigma(n)}=\mathrm{sgn}(\sigma)(e_1\wedge\cdots\wedge e_n).$$

证明 因 $m\wedge m'=-m'\wedge m$，交换积 $e_1\wedge\cdots\wedge e_n$ 中的相邻因子得

$$e_1\wedge\cdots\wedge e_i\wedge e_{i+1}\wedge\cdots\wedge e_n=-e_1\wedge\cdots\wedge e_{i+1}\wedge e_i\wedge\cdots\wedge e_n.$$

更一般地，如果 $i<j$，则可以用一系列相邻因子的交换而交换 e_i 和 e_j，相邻因子每交换一次改变一次符号．根据习题 2.7，这可以用奇数次相邻因子的交换来完成．因此，对任意对换 $\tau\in S_n$，有

$$\begin{aligned}e_{\tau(1)}\wedge\cdots\wedge e_{\tau(n)} &= e_1\wedge\cdots\wedge e_j\wedge\cdots\wedge e_i\wedge\cdots\wedge e_n\\ &=-[e_1\wedge\cdots\wedge e_i\wedge\cdots\wedge e_j\wedge\cdots\wedge e_n]\\ &=\mathrm{sgn}(\tau)(e_1\wedge\cdots\wedge e_n).\end{aligned}$$

对 m 用归纳法证明一般结果，其中 σ 是 m 个对换的积．基础步刚才已经证明．写 $\sigma=\tau_1\tau_2\cdots\tau_{m+1}$，并记 $\tau_2\cdots\tau_{m+1}$为 σ'. 根据归纳假定，

$$e_{\sigma'(1)}\wedge\cdots\wedge e_{\sigma'(n)}=\mathrm{sgn}(\sigma')e_1\wedge\cdots\wedge e_n,$$

759

从而

$$\begin{aligned}e_{\sigma(1)}\wedge\cdots\wedge e_{\sigma(n)} &= e_{\tau_1\sigma'(1)}\wedge\cdots\wedge e_{\tau_1\sigma'(n)}\\ &=-e_{\sigma'(1)}\wedge\cdots\wedge e_{\sigma'(n)} \qquad \text{（基础步）}\end{aligned}$$

$$= -\operatorname{sgn}(\sigma')(e_1\wedge\cdots\wedge e_n) \qquad \text{(归纳步)}$$
$$= \operatorname{sgn}(\tau_1)\operatorname{sgn}(\sigma')(e_1\wedge\cdots\wedge e_n)$$
$$= \operatorname{sgn}(\sigma)(e_1\wedge\cdots\wedge e_n).$$ ■

注 在 k 是域的特殊情形下，这个引理有一个简单的证明．如果 k 有特征 2，则引理 9.152 显然为真，因此可以假定特征不为 2. 设 $e_1,\cdots,e_n$ 是 k^n 的标准基．如果 $\sigma\in S_n$，定义线性变换 $\varphi_\sigma: k^n\to k^n$ 为 $\varphi_\sigma: e_i\mapsto e_{\sigma(i)}$．容易验证 $\varphi_{\sigma\tau}=\varphi_\sigma\varphi_\tau$，因此存在由 $d:\sigma\mapsto\det(\varphi_\sigma)$ 给出的群同态 $d: S_n\to k^\times$．如果 σ 是一个对换，则 $\sigma^2=(1)$ 且在 $k^\times$ 中 $d(\sigma^2)=1$．因 k 是域，$d(\sigma)=\pm1$．因每个置换都是对换的积，从而对每个置换 σ 有 $d(\sigma)=\pm1$，因此，$\operatorname{im}(d)\leqslant\{\pm1\}$．现在只有两个同态 $S_n\to\{\pm1\}$：核为 S_n 的平凡同态和 sgn. 要证明 $d=\operatorname{sgn}$，只需证明 $d((1\ 2))\neq1$．但 $d((1\ 2))=\det(\varphi_{(1\ 2)})$；即，

$$\begin{aligned}\det(\varphi_{(1\ 2)})(e_1\wedge\cdots\wedge e_n) &= \varphi_{(1\ 2)}(e_1)\wedge\cdots\wedge\varphi_{(1\ 2)}(e_n)\\ &= e_2\wedge e_1\wedge e_3\wedge\cdots\wedge e_n\\ &= -(e_1\wedge\cdots\wedge e_n).\end{aligned}$$

因为 k 的特征不为 2，所以 $d((1\ 2))=-1\neq1$，从而对一切 $\sigma\in S_n$，$d(\sigma)=\det(\varphi_\sigma)=\operatorname{sgn}(\sigma)$；即 $e_{\sigma(1)}\wedge\cdots\wedge e_{\sigma(n)}=\operatorname{sgn}(\sigma)(e_1\wedge\cdots\wedge e_n)$.

命题 9.153（完全展开） 设 $e_1,\cdots,e_n$ 是自由 k-模的基，其中 k 是交换环．如果 $A=[a_{ij}]$ 是元素在 k 中的 $n\times n$ 矩阵，则

$$\det(A)=\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)a_{\sigma(1),1}a_{\sigma(2),2}\cdots a_{\sigma(n),n}.$$

证明 展开 A 的列的楔积：

$$\begin{aligned}&\sum_{j_1}a_{j_1 1}e_{j_1}\wedge\sum_{j_2}a_{j_2 2}e_{j_2}\wedge\cdots\wedge\sum_{j_n}a_{j_n n}e_{j_n}\\ &=\sum_{j_1,j_2,\cdots,j_n}a_{j_1 1}e_{j_1}\wedge a_{j_2 2}e_{j_2}\wedge\cdots\wedge a_{j_n n}e_{j_n}.\end{aligned}$$

有 $e_{j_p}=e_{j_q}$ 的任何直和项因为有重复因子，所以必是 0，从而可以假定在任何残存的项中 $j_1,j_2,\cdots,j_n$ 都是不同的；即有某个置换 $\sigma\in S_n$，当 $1\leqslant r\leqslant n$ 时，使得 $j_r=\sigma(r)$．原来的积现在有下面的形式

760

$$\sum_{\sigma\in S_n}a_{\sigma(1)1}a_{\sigma(2)2}\cdots a_{\sigma(n)n}e_{\sigma(1)}\wedge e_{\sigma(2)}\wedge\cdots\wedge e_{\sigma(n)}.$$

根据引理，$e_{\sigma(1)}\wedge e_{\sigma(2)}\wedge\cdots\wedge e_{\sigma(n)}=\operatorname{sgn}(\sigma)(e_1\wedge\cdots\wedge e_n)$．所以，列的楔积等于 $\left(\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)a_{\sigma(1)1}a_{\sigma(2)2}\cdots a_{\sigma(n)n}\right)(e_1\wedge\cdots\wedge e_n)$，证明完成． ■

经常把完全展开作为行列式的定义．

系 9.154 设 k 是交换环，并设 A 是元素在 k 中的 $n\times n$ 矩阵．如果 $u\in k$，则 $\det(uI-A)=f(u)$，其中 $f(x)\in k[x]$ 是 n 次首一多项式．此外，$f(x)$ 中 x^{n-1} 的系数是 $-\operatorname{tr}(A)$．

证明 设 $A=[a_{ij}]$ 和 $B=[b_{ij}]$，其中 $b_{ij}=u\delta_{ij}-a_{ij}$（其中 δ_{ij} 是克罗内克 δ）．根据命题，

$$\det(B)=\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)b_{\sigma(1),1}b_{\sigma(2),2}\cdots b_{\sigma(n),n}.$$

如果 $\sigma=(1)$，则在完全展开式中对应的项是

$$b_{11}b_{22}\cdots b_{nn}=\prod_i(u-a_{ii})=g(u),$$

其中 $g(x)=\prod_i(x-a_{ii})$ 是 $k[x]$ 中 n 次首一多项式．如果 $\sigma\neq(1)$，则在完全展开式中的第 σ 项不

可能恰有 $n-1$ 个因子来自 $uI-A$ 的对角线，这是因为如果 σ 固定 $n-1$ 个指标，则 $\sigma=(1)$．所以，一切 $\sigma\neq(1)$ 的项之和或者是 0，或者是 $k[x]$ 中次数最多是 $n-2$ 的多项式．由此，$\det(f)=n$ 且 x^{n-1} 的系数是 $-\sum_i a_{ii}=-\operatorname{tr}(A)$． ■

命题 9.155 如果 A 是元素在交换环 k 中的 $n\times n$ 矩阵，则

$$\det(A^t)=\det(A),$$

其中 A^t 是 A 的转置．

证明 如果 $A=[a_{ij}]$，把 $\det(A)$ 的完全展开式写得更简洁：

$$\det(A)=\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)\prod_i a_{\sigma(i),i}.$$

因任一置换 $\tau\in S_n$，所以对一切 i 有 $i=\tau(j)$，从而

$$\prod_i a_{\sigma(i),i}=\prod_j a_{\sigma(\tau(j)),\tau(j)},$$

[761]

这不过是重新排列乘积中的因子．选取 $\tau=\sigma^{-1}$ 得

$$\prod_j a_{\sigma(\tau(j)),\tau(j)}=\prod_j a_{j,\sigma^{-1}(j)}.$$

所以，

$$\det(A)=\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)\prod_j a_{j,\sigma^{-1}(j)}.$$

现在 $\operatorname{sgn}(\sigma)=\operatorname{sgn}(\sigma^{-1})$ [如果 $\sigma=\tau_1\cdots\tau_q$，其中 τ 是对换，则 $\sigma^{-1}=\tau_q\cdots\tau_1$]；此外，因为 σ 遍历 S_n，从而 σ^{-1} 也遍历 S_n. 因此，记 $\sigma^{-1}=\rho$ 得

$$\det(A)=\sum_{\rho\in S_n}\operatorname{sgn}(\rho)\prod_j a_{j,\rho(j)}.$$

现在记 $A^t=[b_{ij}]$，其中 $b_{ij}=a_{ji}$，则

$$\det(A^t)=\sum_{\rho\in S_n}\operatorname{sgn}(\rho)\prod_j b_{\rho(j),j}=\sum_{\rho\in S_n}\operatorname{sgn}(\rho)\prod_j a_{j,\rho(j)}=\det(A).$$ ■

我们已经知道元素在域 k 中的 $n\times n$ 矩阵 A 的特征值 $\alpha_1,\cdots,\alpha_n$ 是特征多项式

$$\psi_A(x)=\det(xI-A)\in k[x]$$

的根．我们还知道 $\det(A)=\prod_i\alpha_i$，现在证明 $\operatorname{tr}(A)=\sum_i\alpha_i$．

命题 9.156 如果 $A=[a_{ij}]$ 是元素在域 k 中的 $n\times n$ 矩阵，则

$$\operatorname{tr}(A)=\alpha_1+\alpha_2+\cdots+\alpha_n.$$

证明 在 $\det(xI-A)$ 的完全展开式中，对角线对应于项 $(x-a_{\sigma(1),1})(x-a_{\sigma(2),2})\cdots(x-a_{\sigma(n),n})$，其中 σ 是恒等置换．如果 $\sigma\neq 1$，则至少有两项不在对角线上，从而这个项的次数最多是 $n-2$. 所以，x^{n-1} 在对角线项中的系数 b_{n-1} 是 $-\sum_i a_{ii}$，和 $\psi_A(x)$ 中的 x^{n-1} 的系数一致，即 $-\sum_i\alpha_i=-\operatorname{tr}(A)$，其中 $\alpha_1,\cdots,\alpha_n$ 是 A 的特征值．另一方面，

$$\psi_A(x)=\prod_i(x-\alpha_i),$$

从而正如所求，x^{n-1} 的系数是 $-\sum_i\alpha_i$． ■

我们知道相似矩阵有相同的行列式和相同的迹．下一个系推广了这个事实，因为它们的特征多

762 项式的一切系数都一致.

系 9.157 如果 A 和 B 是元素在域 k 中的 $n\times n$ 相似矩阵，则 A 和 B 有相同的特征多项式.

证明 存在非奇异矩阵 P 使得 $B=PAP^{-1}$，且

$$\begin{aligned}\psi_B(x) &= \det(xI-B)\\ &= \det(xI-PAP^{-1})\\ &= \det(P(xI-A)P^{-1})\\ &= \det(P)\det(xI-A)\det(P)^{-1}\\ &= \det(xI-A)\\ &= \psi_A(x).\end{aligned}$$

■

定义 设 A 是元素在交换环 k 中的 $n\times n$ 矩阵. 如果 $H=i_1,\cdots,i_p$ 和 $L=j_1,\cdots,j_p$ 是递增 $p\leqslant n$-表，则 A_{HL} 是指 $p\times p$ **子矩阵** $[a_{st}]$，其中 $(s,t)\in H\times L$. 一个 p **阶子式**是指一个 $p\times p$ 子矩阵的行列式.

例如，每个元素 a_{ij} 都是 $A=[a_{ij}]$的 1 阶子式. 如果

$$A=\begin{bmatrix}a_{11} & a_{12} & a_{13}\\ a_{21} & a_{22} & a_{23}\\ a_{31} & a_{32} & a_{33}\end{bmatrix},$$

则某个 2 阶子式是

$$\det\begin{bmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{bmatrix}\text{和 }\det\begin{bmatrix}a_{12} & a_{13}\\ a_{32} & a_{33}\end{bmatrix}.$$

特别地，如果 $1\leqslant i\leqslant n$，令 i' 表示递增 $n-1\leqslant n$-表，其中删去 i；于是 $(n-1)\times(n-1)$ 子矩阵形如 $A_{i'j'}$，它的行列式是 $n-1$ 阶子式. 注意 $A_{i'j'}$ 是在 A 中删去第 i 行和第 j 列得到的子矩阵.

引理 9.158 设 k 是交换环，并把 $x_{i_1},\cdots,x_{i_p}\in k^n$ 看作一个 $n\times p$ 矩阵 A 的列，其中 $H=i_1,\cdots,i_p$ 是一个递增 $p\leqslant n$-表. 则

$$x_{i_1}\wedge\cdots\wedge x_{i_p}=\sum_L\det(A_{L,H})e_L,$$

其中 L 遍历一切递增 $p\leqslant n$-表.

证明 对 $\ell=1,2,\cdots,p$, 记 $x_{i_\ell}=\sum_{t_\ell}a_{t_\ell i_\ell}e_{t_\ell}$，从而

$$\begin{aligned}x_{i_1}\wedge\cdots\wedge x_{i_p} &= \sum_{t_1}a_{t_1i_1}e_{t_1}\wedge\cdots\wedge\sum_{t_p}a_{t_pi_p}e_{t_p}\\ &= \sum_{t_1\cdots t_p}a_{t_1i_1}\cdots a_{t_pi_p}e_{t_1}\wedge\cdots\wedge e_{t_p}.\end{aligned}$$

763

包含重复下标的项都是 0，因此可以假定这个和是一切无重复 $t_1,\cdots,t_p$ 上的和；即 $\{1,2,\cdots,n\}$ 的一切 p-子表 $T=\{t_1,\cdots,t_p\}$ 上的和. 合并同类项，可以把和重写作

$$\sum_T\sum_{T=\{t_1,\cdots,t_p\}}a_{t_1i_1}\cdots a_{t_pi_p}e_{t_1}\wedge\cdots\wedge e_{t_p}.$$

对任意固定的 p-子表 $T=\{t_1,\cdots,t_p\}$，设 $L=\ell_1,\ell_2,\cdots,\ell_p$ 是 T 中整数组成的递增 p-表；于是存在置换 $\sigma\in S_p$ 使得 $\ell_{\sigma(1)}=t_1,\cdots,\ell_{\sigma(p)}=t_p$，利用这个记号，

$$\sum_{T=\{t_1,\cdots,t_p\}}a_{t_1i_1}\cdots a_{t_pi_p}(e_{t_1}\wedge\cdots\wedge e_{t_p})=\sum_{\sigma\in S_p}a_{\ell_{\sigma(1)}i_1}\cdots a_{\ell_{\sigma(p)}i_p}(e_{t_1}\wedge\cdots\wedge e_{t_p})$$

$$= \sum_{\sigma \in S_p} \operatorname{sgn}(\sigma) a_{\ell_{\sigma(1)} i_1} \cdots a_{\ell_{\sigma(p)} i_p} e_L$$
$$= \det(A_{L,H}) e_L. \quad \blacksquare$$

外代数 $\bigwedge(V)$ 中的乘法由基元素对的乘积 $e_H \wedge e_K$ 确定．我们引入下面的记号：如果 $H = t_1, \cdots, t_p$ 和 $K = \ell_1, \cdots, \ell_q$ 是不相交递增表，则定义 $\tau_{H,K}$ 为把表 $t_1, \cdots, t_p, \ell_1, \cdots, \ell_q$ 重排成递增表的置换，记为 $H * K$. 定义

$$\rho_{H,K} = \operatorname{sgn}(\tau_{H,K}).$$

用这个记号，引理 9.152 说

$$e_H \wedge e_K = \begin{cases} 0 & \text{如果 } H \cap K \neq \varnothing \\ \rho_{H,K} e_{H * K} & \text{如果 } H \cap K = \varnothing. \end{cases}$$

例 9.159 如果 $H = 1, 3, 4$ 和 $K = 2, 6$ 都是递增表，则

$$H * K = 1,2,3,4,6$$

和

$$\tau_{H,K} = \begin{pmatrix} 1 & 3 & 4 & 2 & 6 \\ 1 & 2 & 3 & 4 & 6 \end{pmatrix} = (2\ 4\ 3).$$

所以，

$$\rho_{H,K} = \operatorname{sgn} \tau_{H,K} = +1$$

和

$$e_H \wedge e_K = (e_1 \wedge e_3 \wedge e_4) \wedge (e_2 \wedge e_6) = e_1 \wedge e_2 \wedge e_3 \wedge e_4 \wedge e_6 = e_{H * K}. \quad \blacksquare$$

764

命题 9.160 设 $A = [a_{ij}]$ 是元素在交换环 k 中的 $n \times n$ 矩阵．

（i）如果 $I = i_1, \cdots, i_p$ 是递增 p-表且 $x_{i_1}, \cdots, x_{i_p}$ 是 A 的对应的列，则记 $x_{i_1} \wedge \cdots \wedge x_{i_p}$ 为 x_I. 如果 $J = j_1, \cdots, j_q$ 是递增 q-表，则

$$x_I \wedge x_J = \sum_{H,K} \rho_{H,K} \det(A_{H,I}) \det(A_{K,J}) e_{H * K},$$

其中 $H * K$ 是当 $H \cap K = \varnothing$ 时由 $H \cup K$ 形成的递增 $(p+q)$-表．

（ii）按第 j 列的拉普拉斯[⊖]展开：对每个固定的 j,

$$\det(A) = (-1)^{1+j} a_{1j} \det(A_{1'j'}) + \cdots + (-1)^{n+j} a_{nj} \det(A_{n'j'}),$$

其中 $A_{i'j'}$ 是从 A 中删去第 i 行和第 j 列得到的 $(n-1) \times (n-1)$ 子矩阵．

（iii）按第 i 行的拉普拉斯展开：对每个固定的 i,

$$\det(A) = (-1)^{i+1} a_{i1} \det(A_{i'1'}) + \cdots + (-1)^{i+n} a_{in} \det(A_{i'n'}).$$

证明 （i）根据引理，

$$\begin{aligned} x_I \wedge x_J &= \sum_H \det(A_{H,I}) e_H \wedge \sum_K \det(A_{K,J}) e_K \\ &= \sum_{H,K} \det(A_{H,I}) e_H \wedge \det(A_{K,J}) e_K \\ &= \sum_{H,K} \det(A_{H,I}) \det(A_{K,J}) e_H \wedge e_K \\ &= \sum_{H,K} \rho_{H,K} \det(A_{H,I}) \det(A_{K,J}) e_{H * K}. \end{aligned}$$

⊖ 以拉普拉斯的名字命名．

（ii）如果 $I=j$ 只有一个元素，$J=j'=1,\cdots,\hat{j},\cdots,n$ 是它的补集，则因为 $j,1,\cdots,\hat{j},\cdots,n$ 可用 $j-1$ 个对换排成升序，所以

$$\begin{aligned}x_j \wedge x_{j'} &= x_j \wedge x_1 \wedge \cdots \wedge \hat{x}_j \wedge \cdots \wedge x_n \\ &= (-1)^{j-1} x_1 \wedge \cdots \wedge x_n \\ &= (-1)^{j-1} \det(A) e_1 \wedge \cdots \wedge e_n,\end{aligned}$$

另一方面，用（i）可计算 $x_j \wedge x_{j'}$：

765

$$x_j \wedge x_{j'} = \sum_{H,K} \rho_{H,K} \det(A_{H,j}) \det(A_{K,j'}) e_{H*K}.$$

在这个和中，H 只有一个元素，比如 $H=i$，而 K 有 $n-1$ 个元素；于是，有某个元素ℓ使得 $K=\ell'$. 因当 $\{i\}\cap\ell' \neq \varnothing$ 时有 $e_h \wedge e_\ell = 0$，我们可以假定 $i \notin \ell'$；即可以假定$\ell' = i'$. 现在，$\det(A_{i,j}) = a_{ij}$（这是 1×1 子式），而 $\det(A_{K,j'}) = \det(A_{i'j'})$；即 $A_{i'j'}$ 是从 A 中删去第 j 列和第 i 行得到的子矩阵. 因此，如果 $e_N = e_1 \wedge \cdots \wedge e_n$，则

$$\begin{aligned}x_j \wedge x_{j'} &= \sum_{H,K} \rho_{H,K} \det(A_{H,j}) \det(A_{K,j'}) e_{H*K} \\ &= \sum_i \rho_{i,i'} \det(A_{ij}) \det(A_{i'j'}) e_N \\ &= \sum_i (-1)^{i-1} a_{ij} \det(A_{i'j'}) e_N.\end{aligned}$$

所以，由 $x_j \wedge x_{j'}$ 的两个值相等得

$$\det(A) = \sum_i (-1)^{i+j} a_{ij} \det(A_{i'j'}),$$

正如所求.

（iii）按 A 的第 i 行的拉普拉斯展开是按 A^t 的第 i 列的拉普拉斯展开，因为 $\det(A^t)=\det(A)$，从而得到结论. ■

注意，我们已经证明按任一行或任一列的拉普拉斯展开都有相同的值；即行列式不依赖于用来展开的行或列. 拉普拉斯展开类似于矩阵乘法形成的和，下面造出的矩阵使得这种类似成为事实.

定义 如果 $A=[a_{ij}]$是元素在交换环 k 中的 $n\times n$ 矩阵，则 A 的**伴随矩阵**⊖是

$$\operatorname{adj}(A) = [C_{ij}],$$

其中

$$C_{ij} = (-1)^{i+j} \det(A_{j'i'}).$$

下标的倒置是有意的. 就是说，$\operatorname{adj}(A)$是 ij 元素为$(-1)^{i+j}\det(A_{i'j'})$的矩阵的转置. 我们常称 C_{ij} 为 A 的 **ij-余子式**.

系 9.161 如果 A 是元素在交换环 k 中的 $n\times n$ 矩阵，则

766

$$A\operatorname{adj}(A) = \det(A) I = \operatorname{adj}(A) A.$$

证明 记 $A\operatorname{adj}(A)$的 ij 元素为 b_{ij}. 矩阵乘法的定义给出

$$b_{ij} = \sum_{p=1}^{n} a_{ip} C_{pj} = \sum_{p=1}^{n} a_{ip} (-1)^{j+p} \det(A_{j'p'}).$$

如果 $j=i$，则命题 9.160 给出

$$b_{ii} = \det(A).$$

⊖ 刚才定义的伴随矩阵和定义在内积空间上的伴随矩阵之间没有联系.

如果 $j\neq i$，考虑把 A 的 j 行换成 i 行而得到的矩阵 M. 当然，因为 M 有两个相同的行，所以 $\det(M)=0$. 另一方面，可以按它的“新的” j 行用拉普拉斯展开来计算 $\det(M)$. 一切子矩阵 $M_{j'p'}=A_{j'p'}$，且 M 和 A 的一切对应余子式都相等. 这个矩阵的新的 j 行的元素是 a_{ip}，从而

$$0=\det(M)=(-1)^{i+1}a_{i1}\det(A_{j'1'})+\cdots+(-1)^{i+n}a_{in}\det(A_{j'n'}).$$

我们已经证明了 $A\,\mathrm{adj}(A)$ 是一个对角矩阵，它的每个对角线元素都等于 $\det(A)$.

$\det(A)I=\mathrm{adj}(A)A$ 的证明是类似的，留给读者. [也可以修改系 3.107 的证明，只要把向量空间换成自由 k-模，或者可以证明 $\mathrm{adj}(A^t)=\mathrm{adj}(A)^t$.] ■

定义 设 A 是元素在交换环 k 中的 $n\times n$ 矩阵，如果存在元素在 k 中的矩阵 B 使得

$$AB=I=BA,$$

则称 A **在 k 上可逆**.

如果 k 是域，则可逆矩阵常称作**非奇异的**，且用行列式非零来刻画. 考虑元素在$\mathbb{Z}$中的矩阵：

$$A=\begin{bmatrix}3&1\\1&1\end{bmatrix}.$$

现在 $\det(A)=2\neq 0$，但它在$\mathbb{Z}$上不是可逆的. 假设

$$\begin{bmatrix}3&1\\1&1\end{bmatrix}\begin{bmatrix}a&c\\b&d\end{bmatrix}=\begin{bmatrix}3a+b&3c+d\\a+b&c+d\end{bmatrix}.$$

如果这个积是 I，则

$$3a+b=1=c+d$$
$$3c+d=0=a+b.$$

因此，$b=-a$ 和 $1=3a+b=2a$；因为在$\mathbb{Z}$中 $1=2a$ 无解，矩阵 A 在$\mathbb{Z}$上不是可逆的. 当然，A 在$\mathbb{Q}$上可逆.

767

命题 9.162 如果 k 是交换环且 $A\in\mathrm{Mat}_n(k)$，则 A 是可逆的当且仅当 $\det(A)$ 是 k 中的单位.

证明 如果 A 是可逆的，则存在矩阵 B 使得 $AB=I$. 因此，

$$1=\det(I)=\det(AB)=\det(A)\det(B);$$

这就是说 $\det(A)$ 是 k 中的单位.

反之，假定 $\det(A)$ 是 k 中的单位，从而存在元素 $u\in k$ 使得 $u\det(A)=1$. 定义

$$B=u\,\mathrm{adj}(A).$$

根据系 9.161，

$$AB=Au\,\mathrm{adj}(A)=u\det(A)I=I=u\,\mathrm{adj}(A)A=BA.$$

于是，A 是可逆的. ■

下面是用外代数证明用分块形式计算矩阵的行列式的方法.

命题 9.163 设 k 是交换环，并设

$$X=\begin{bmatrix}A&C\\0&B\end{bmatrix}$$

是元素在 k 中的 $(m+n)\times(m+n)$ 矩阵，其中 A 是一个 $m\times m$ 子矩阵，B 是一个 $n\times n$ 子矩阵. 则

$$\det(X)=\det(A)\det(B).$$

证明 设 $e_1,\cdots,e_{m+n}$ 是 k^{m+n} 的标准基，设 $\alpha_1,\cdots,\alpha_m$ 是 A 的列向量（它也是 X 的前 m 个列向量），并设 $\gamma_i+\beta_i$ 是 X 的第 $(m+i)$ 个列向量，其中 γ_i 是 C 的第 i 个列向量和 β_i 是 B 的第 i 个列向量.

现在 $\gamma_i \in \langle e_1, \cdots, e_m \rangle$，从而 $\gamma_i = \sum_{j=1}^{m} c_{ji} e_j$．所以，如果 $H = 1,2,\cdots,n$，则

$$e_H \wedge \gamma_i = e_H \wedge \sum_{j=1}^{m} c_{ji} e_j = 0,$$

这是因为每个项中 e_j 有重复．用结合性，我们知道

$$\begin{aligned} e_H \wedge (\gamma_1 + \beta_1) \wedge (\gamma_2 + \beta_2) \wedge \cdots \wedge (\gamma_n + \beta_n) &= e_H \wedge \beta_1 \wedge (\gamma_2 + \beta_2) \wedge \cdots \wedge (\gamma_n + \beta_n) \\ &= e_H \wedge \beta_1 \wedge \beta_2 \wedge \cdots \wedge (\gamma_n + \beta_n) \\ &= e_H \wedge \beta_1 \wedge \beta_2 \wedge \cdots \wedge \beta_n. \end{aligned}$$

768

因此，如果 $J = m+1, m+2, \cdots, m+n$，

$$\begin{aligned} \det(X) e_H \wedge e_J &= \alpha_1 \wedge \cdots \wedge \alpha_m \wedge (\gamma_1 + \beta_1) \wedge \cdots \wedge (\gamma_n + \beta_n) \\ &= \det(A) e_H \wedge (\gamma_1 + \beta_1) \wedge \cdots \wedge (\gamma_n + \beta_n) \\ &= \det(A) e_H \wedge \beta_1 \wedge \cdots \wedge \beta_n \\ &= \det(A) e_H \wedge \det(B) e_J \\ &= \det(A)\det(B) e_H \wedge e_J. \end{aligned}$$

所以，$\det(X) = \det(A)\det(B)$. ■

系 9.164 如果 $A = [a_{ij}]$ 是 $n \times n$ 三角矩阵，即对一切 $i < j$，$a_{ij} = 0$，（下三角）或对一切 $i > j, a_{ij} = 0$（上三角），则

$$\det(A) = \prod_{i=1}^{n} a_{ii};$$

即 $\det(A)$ 是对角线元素的积．

证明 容易对 $n \geqslant 1$ 用归纳法证明，用按第一列拉普拉斯展开（对上三角矩阵），并用命题证明归纳步． ■

虽然用矩阵 A 的列的楔积定义的 A 的行列式给出了计算行列式的一个明显的算法，但是当 A 的元素在一个域中的时候，有计算 $\det(A)$ 更有效的方法．用高斯消元法，通过初等行运算把 A 变成一个上三角矩阵 T：

$$A \to A_1 \to \cdots \to A_r = T.$$

记录所用的运算．例如，如果 $A \to A_1$ 是 Ⅰ 型运算，它是用单位 c 乘一行，则 $c\det(A) = \det(A_1)$，从而 $\det(A) = c^{-1}\det(A_1)$；如果 $A \to A_1$ 是 Ⅱ 型运算，它是某行的一个倍数加到另一行，则 $\det(A) = \det(A_1)$；如果 $A \to A_1$ 是 Ⅲ 型运算，它交换两行，则 $\det(A) = -\det(A_1)$．于是，最终可以根据记录下的运算把 $\det(A)$ 用 $\det(T)$ 写出来．但因 T 是上三角矩阵，所以 $\det(T)$ 是对角线元素的积．

外代数的另一个应用是构造映射的迹．

定义 设 k 是交换环，并设 A 是 k-代数．A 的**导子**是 k-模的同态 $d: A \to A$ 满足

$$d(ab) = (da)b + a(db).$$

769

就是说，导子和微积分中通常定义的微分有类似的作用，即乘法法则 $(fg)' = f'g + fg'$ 成立．

引理 9.165 设 k 是交换环，并设 M 是 k-模．

（ⅰ）如果 $\varphi: M \to M$ 是 k-映射，则存在唯一的导子 $D_\varphi: T(M) \to T(M)$，它是一个分次映射（次数为 0）满足 $D_\varphi | M = \varphi$，其中 $T(M)$ 是 M 上的张量代数；即对一切 $p \geqslant 0$，

$$D_\varphi(T^p(M)) \subseteq T^p(M).$$

（ⅱ）如果 $\varphi: M \to M$ 是 k-映射，则存在唯一的导子 $d_\varphi: \bigwedge(M) \to \bigwedge(M)$，它是分次映射（次数为 0）满足 $d_\varphi \mid M = \varphi$；即对一切 $p \geqslant 0$，

$$d_\varphi(\bigwedge^p(M)) \subseteq \bigwedge^p(M).$$

证明 （ⅰ）定义 $D_\varphi \mid k = 1_k$（回忆 $T^0(M) = k$），并定义 $D_\varphi \mid T^1(M) = \varphi$（回忆 $T^1(M) = M$）. 如果 $p \geqslant 2$，定义 $D_\varphi^p: T^p(M) \to T^p(M)$ 为

$$D_\varphi^p(m_1 \otimes \cdots \otimes m_p) = \sum_{i=1}^p m_1 \otimes \cdots \otimes \varphi(m_i) \otimes \cdots \otimes m_p.$$

对每个 i，和式中的第 i 个直和项是合理定义的，这是因为它由 k-多重线性函数 $(m_1, \cdots, m_p) \mapsto m_1 \otimes \cdots \otimes \varphi(m_i) \otimes \cdots \otimes m_p$ 形成；由此，D_φ 是合理定义的.

显然 D_φ 是 k-模的映射. 要验证 D_φ 是导子，只要考虑它在齐次元素 $u = u_1 \otimes \cdots \otimes u_p$ 和 $v = v_1 \otimes \cdots \otimes v_q$ 上的作用.

$$\begin{aligned} D_\varphi(uv) &= D_\varphi(u_1 \otimes \cdots \otimes u_p \otimes v_1 \otimes \cdots \otimes v_q) \\ &= \sum_{i=1}^p u_1 \otimes \cdots \otimes \varphi(u_i) \otimes \cdots \otimes u_p \otimes v \\ &\quad + \sum_{j=1}^q u \otimes v_1 \otimes \cdots \otimes \varphi(v_j) \otimes \cdots \otimes v_q \\ &= D_\varphi(u)v + uD_\varphi(v). \end{aligned}$$

唯一性的证明留给读者.

（ⅱ）用与 D_φ 相同的公式定义 $d_\varphi: \bigwedge(M) \to \bigwedge(M)$，只是把$\otimes$改为$\wedge$. 为证明这是合理定义的，需要证明 $D_\varphi(J) \subseteq J$，其中 J 是由形如 $m \otimes m$ 的一切元素生成的双边理想. 只需对 $p \geqslant 2$ 用归纳法证明 $D_\varphi(J^p) \subseteq J$，其中 $J^p = J \cap T^p(M)$. 基础步 $p = 2$ 来自下列恒等式，对 $a, b \in M$，

$$a \otimes b + b \otimes a = (a+b) \otimes (a+b) - a \otimes a - b \otimes b \in J.$$

770

归纳步来自下列恒等式，对 $a, c \in M$ 和 $b \in J^{p-1}$，

$$\begin{aligned} a \otimes b \otimes c + J &= -a \otimes c \otimes b + J \\ &= c \otimes a \otimes b + J \\ &= -c \otimes b \otimes a + J. \end{aligned}$$

■

命题 9.166 设 k 是交换环，并设 M 是以 $e_1, \cdots, e_n$ 为基的有限生成自由 k-模. 如果 $\varphi: M \to M$ 是 k-映射且 $d_\varphi: \bigwedge(M) \to \bigwedge(M)$ 是由它确定的导子，则

$$d_\varphi \mid \bigwedge^n(M) = \mathrm{tr}(\varphi) e_L,$$

其中 $e_L = e_1 \wedge \cdots \wedge e_n$.

证明 根据引理 9.165（ⅱ），有 $d_\varphi: \bigwedge^n(M) \to \bigwedge^n(M)$. 因 M 是秩为 n 的自由 k-模，二项式定理给出 $\bigwedge^n(M) \cong k$. 因此有某个 $c \in k$ 使得 $d_\varphi(e_L) = ce_L$；我们现在证明 $c = \mathrm{tr}(\varphi)$. 现在 $\varphi(e_i) = \sum a_{ji} e_j$.

$$\begin{aligned} d_\varphi(e_L) &= \sum_r e_1 \wedge \cdots \wedge \varphi(e_r) \wedge \cdots \wedge e_n \\ &= \sum_r e_1 \wedge \cdots \wedge \sum a_{jr} e_j \wedge \cdots \wedge e_n \\ &= \sum_r e_1 \wedge \cdots \wedge a_{rr} e_r \wedge \cdots \wedge e_n \\ &= \sum_r a_{rr} e_L \\ &= \operatorname{tr}(\varphi) e_L. \end{aligned}$$

■

习题

9.95 设 k 是交换环，并设 V 和 W 是秩分别为 m 和 n 的自由 k-模．

（i）证明：如果 $f: V \to V$ 是 k-映射，则

$$\det(f \otimes 1_W) = [\det(f)]^n.$$

（ii）证明：如果 $f: V \to V$ 和 $g: W \to W$ 都是 k-映射，则

771

$$\det(f \otimes g) = [\det(f)]^n [\det(g)]^m.$$

9.96 （i）设 $z_1, \cdots, z_n$ 是交换环 k 中的元素，考虑范德蒙德矩阵

$$V(z_1, \cdots, z_n) = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ z_1 & z_2 & \cdots & z_n \\ z_1^2 & z_2^2 & \cdots & z_n^2 \\ \vdots & \vdots & \vdots & \vdots \\ z_1^{n-1} & z_2^{n-1} & \cdots & z_n^{n-1} \end{bmatrix}.$$

证明 $\det(V(z_1, \cdots, z_n)) = \prod_{i<j} (z_j - z_i)$．

（ii）如果 $f(x) = \prod_i (x - z_i)$ 有判别式 D，证明 $D = \det(V(z_1, \cdots, z_n))$．

（iii）证明：如果 $z_1, \cdots, z_n$ 是域 k 中不同的元素，则 $V(z_1, \cdots, z_n)$ 是非奇异的．

9.97 定义三对角矩阵是形如

$$T[x_1, \cdots, x_n] = \begin{bmatrix} x_1 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ -1 & x_2 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & -1 & x_3 & 1 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & x_4 & \cdots & 0 & 0 & 0 & 0 \\ & \vdots & & & \ddots & & \vdots & & \\ 0 & 0 & 0 & 0 & \cdots & x_{n-3} & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & -1 & x_{n-2} & 1 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & -1 & x_{n-1} & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & -1 & x_n \end{bmatrix}$$

的 $n \times n$ 矩阵．

（i）如果 $D_n = \det(T[x_1, \cdots, x_n])$，证明 $D_1 = x_1, D_2 = x_1 x_2 + 1$，且对一切 $n > 2$，

$$D_n = x_n D_{n-1} + D_{n-2}.$$

（ii）证明：如果一切 $x_i = 1$，则 $D_n = F_{n+1}$，它是第 n 个斐波那契数．（回忆 $F_0 = 0, F_1 = 1$，对一切 $n \geq 2, F_n = F_{n-1} + F_{n-2}$．）

9.98 如果矩阵 A 是方块的直和，

$$A = B_1 \oplus \cdots \oplus B_t,$$

证明 $\det(A) = \prod_i \det(B_i)$.

9.99 如果 A 和 B 都是元素在交换环 R 中的 $n \times n$ 矩阵，证明 AB 和 BA 有相同的特征多项式.

提示：(Goodwillie)

$$\begin{bmatrix} I & B \\ 0 & I \end{bmatrix}\begin{bmatrix} 0 & 0 \\ A & AB \end{bmatrix}\begin{bmatrix} I & -B \\ 0 & I \end{bmatrix} = \begin{bmatrix} BA & 0 \\ A & 0 \end{bmatrix}.$$

9.10 李代数

非结合代数有一些重要的例子，其中最重要的是李代数. 19 世纪末，Sophus Lie（读作李）研究了偏微分方程组的解空间 S，使用了 S 的变换群 G. G 的底集是一个微分流形，群运算是一个 C^∞-函数；这样的群叫做李群. 解空间与它的李群 G 密切相关；G 是用它的李代数来研究的，这是一个相当简单的对象，缘起于 G 的幺元处的切空间. 对于它们的研究，除了这个基本原因之外，李代数成为处理向量空间上的线性变换族的合适方法（与本章前几节给出的单一线性变换的典范型的研究相对照）. 此外，在 19 世纪到 20 世纪的交替之时，属于基灵（W. Killing）和嘉当的单有限维复李代数的分类成为最近一切有限单群的分类的模型，谢瓦莱（C. Chevalley）认识到可以通过模仿单李代数的构造来构造有限单群的类似的族. 772

在给出李代数的定义之前，先给出一个相关的定义. 我们已经定义了环的导子；现在对这个概念稍作推广.

定义 设 k 是交换环. 一个**未必结合的 k-代数** A 是指一个 k-代数配置了某个乘法 $A \times A \to A$，记为 $(a,b) \mapsto ab$，满足

（i）对一切 $a,b,c \in A$, $a(b+c) = ab + ac$ 和 $(b+c)a = ba + ca$；

（ii）对一切 $u \in k$ 和 $a \in A$, $ua = au$；

（iii）对一切 $u \in k$ 和 $a,b \in A$, $a(ub) = (au)b = u(ab)$.

A 的**导子**是指一个 k-映射 $d: A \to A$ 满足

$$d(ab) = (da)b + a(db).$$

微积分中常微分是一个导子，这是因为乘法法则成立，$(fg)' = f'g + fg'$，除此以外，一切多元实值函数 $f(x_1, \cdots, x_n)$ 的 $\mathbb{R}$-代数 A 提供了另一个例子. 对 $i = 1, \cdots, n$ 偏导数 $\partial / \partial x_i$ 是导子.

两个导子的复合未必是导子. 例如，如果 $d: A \to A$ 是导子，则 $d^2 = d \circ d: A \to A$ 满足等式

$$d^2(fg) = d^2(f)g + 2d(f)d(g) + fd^2(g);$$

混合项 $2d(f)d(g)$ 是 d^2 成为导子的障碍. 更一般地，可以把莱布尼茨公式（习题 1.6）从一切 C^∞-函数的环上的常微分推广到任意未必结合的代数 A 上的导子. 如果 $f,g \in A$，则

$$d^n(fg) = \sum_{i=0}^{n} \binom{n}{i} d^i f \cdot d^{n-i} g.$$

773

计算两个导子 d_1 和 d_2 的复合仍然是有价值的. 如果 A 是一个未必结合的代数且 $f,g \in A$，则

$$\begin{aligned} d_1 d_2(fg) &= d_1[(d_2 f)g + f(d_2 g)] \\ &= (d_1 d_2 f)g + (d_2 f)(d_1 g) + (d_1 f)(d_2 g) + f(d_1 d_2 g). \end{aligned}$$

当然，

$$d_2d_1(fg)=(d_2d_1f)g+(d_1f)(d_2g)+(d_2f)(d_1g)+f(d_2d_1g).$$

如果记 $d_1d_2-d_2d_1$ 为$[d_1,d_2]$，代入得

$$[d_1,d_2](fg)=([d_1,d_2]f)g+f([d_1,d_2]g);$$

即$[d_1,d_2]=d_1d_2-d_2d_1$是一个导子．

例 9.167　如果 k 是交换环，对 $\mathrm{Mat}_n(k)$ 配置**方括号运算**：

$$[A,B]=AB-BA.$$

当然，A 和 B 交换当且仅当$[A,B]=0$. 容易举例证明方括号运算是不结合的．然而，对任意固定的 $n\times n$ 矩阵 M，定义为

$$\mathrm{ad}_M: A\mapsto[M,A]$$

的函数

$$\mathrm{ad}_M:\mathrm{Mat}_n(k)\to\mathrm{Mat}_n(k)$$

是一个导子：

$$[M,[A,B]]=[[M,A],B]+[A,[M,B]].$$

这个恒等式的验证需要一个人毕生的时间． ■

李代数的定义涉及一个带有推广"方括号"的乘法的向量空间．

定义　如果 k 是域，则 k 上的一个**李代数**是指 k 上的一个向量空间 L，它配置有双线性运算 $L\times L\to L$，记为 $(a,b)\mapsto[a,b]$（叫做**方括号运算**），满足

（i）对一切 $a\in L,[a,a]=0$；

774

（ii）对每个 $a\in L$，函数 $\mathrm{ad}_a: b\mapsto[a,b]$ 是导子．

对一切 $u,v\in L$，双线性性给出

$$[u+v,u+v]=[u,u]+[u,v]+[v,u]+[v,v],$$

结合第一个公理 $[a,a]=0$，得

$$[u,v]=-[v,u];$$

即方括号乘法是**反交换**的．第二个公理常写得更详细．如果 $b,c\in L$，则它们在 L 中的乘积记为 $[b,c]$；ad_a 是导子就是说

$$[a,[b,c]]=[[a,b],c]+[b,[a,c]];$$

重写得

$$[a,[b,c]]-[b,[a,c]]-[[a,b],c]=0.$$

现在从第一个公理得到的反交换性给出**雅可比恒等式**：

$$\text{对一切 } a,b,c\in L,[a,[b,c]]+[b,[c,a]]+[c,[a,b]]=0$$

于是，一个向量空间 L 是一个李代数当且仅当对一切 $a\in L,[a,a]=0$，且雅可比恒等式成立．

下面是李代数的一些例子．

例 9.168　（i）如果 V 是域 k 上的向量空间，对一切 $a,b\in V$，定义 $[a,b]=0$．显然如此配置的 V 是一个李代数，它叫做**阿贝尔李代数**．

（ii）在$\mathbb{R}^3$ 中，定义 $[u,v]=u\times v$，这是微积分中定义的向量积（或叉积）．容易验证 $v\times v=0$ 且雅可比恒等式成立，从而$\mathbb{R}^3$ 是一个李代数．这个例子可以推广：对每个域 k，可以在向量空间 k^3 上定义叉积从而使它成为一个李代数．

(iii) 域 k 上的李代数 L 的一个**子代数** S 是指在方括号运算下封闭的子空间：如果 $a,b\in S$，则 $[a,b]\in S$. 易知每个子代数自身都是李代数.

(iv) 如果 k 是域，定义方括号运算为

$$[A,B]=AB-BA,$$

则 $\mathrm{Mat}_n(k)$ 是李代数. 我们常记这个李代数为 $\mathfrak{gl}(n,k)$. 这个例子是非常一般的，因为阿多 (I. D. Ado) 的一个定理说对特征为 0 的域 k 上的每个有限维李代数对某个 n 同构于 $\mathfrak{gl}(n,k)$ 的一个子代数.（见 Jacobson 所著的《Lie Algebras》，202 页）.

(v) $\mathfrak{gl}(n,k)$ 的一个重要的子代数是 $\mathfrak{sl}(n,k)$，它由一切迹为 0 的 $n\times n$ 矩阵组成. 事实上，如果 G 是李群，它的相伴李代数是 $\mathfrak{g}$，则存在类似取幂的 $\mathfrak{g}\to G$. 特别地，如果 $\mathfrak{g}=\mathfrak{gl}(n,\mathbb{C})$，则这个映射是取幂 $A\mapsto e^A$. 于是，命题9.52(viii)表明取幂把 $\mathfrak{sl}(n,\mathbb{C})$ 送入 $\mathrm{SL}(n,\mathbb{C})$. 775

(vi) 如果 A 是域 k 上的任一代数，则

$$\mathfrak{Der}(A/k)=\{\text{一切导子 } d: A\to A\}$$

(具有方括号运算$[d_1,d_2]=d_1d_2-d_2d_1$)是一个李代数.

由莱布尼茨法则，如果 k 的特征 $p>0$，则对每个 $d\in\mathfrak{Der}(A/k)$，d^p 是导子，因为只要 $0<i<p$，就有 $\binom{p}{i}\equiv 0 \bmod p$.（这是叫做特征 p 的**限制李代数**的一例.）

对某种纯不可分扩张有一个伽罗瓦理论，它属于雅各布森（见 Jacobson 所著的《Basic Algebra II》，533～536 页）. 如果 k 是特征 $p>0$ 的域，且 E/k 是高为 1 的有限纯不可分扩张，即对一切 $\alpha\in E$，$\alpha^p\in k$，则在一切中间域的族和$\mathfrak{Der}(E/k)$ 的限制李子代数之间存在一一映射，它由

$$B\mapsto\mathfrak{Der}(E/B)$$

给出；这个函数的逆由

$$\mathfrak{L}\mapsto\{e\in E: D(e)=0 \text{ 对一切 } D\in\mathfrak{L}\}$$

给出. ■

并不奇怪，域 k 上的一切李代数形成一个范畴.

定义 如果 L 和 L' 都是域 k 上的李代数，则称函数 $f: L\to L'$ 为**李同态**，如果 f 是保持方括号运算的 k-线性变换：对一切 a，$b\in L$，

$$f([a,b])=[fa,fb].$$

定义 李代数 L 的**理想**是一个子空间 I 满足对每个 $x\in L$ 和 $a\in I$ 有$[x,a]\in I$.

即使李代数未必交换，它的反交换性也表明每个左理想（如刚才定义的）必是右理想；即每个理想都是双边理想.

称李代数 L 为**单的**，如果 $L\neq\{0\}$且 L 没有非零真理想.

定义 如果 I 是 L 中的理想，则**商** L/I 是指商空间（把 L 看作向量空间并把 I 看作子空间），其方括号运算由

$$[a+I,b+I]=[a,b]+I$$

定义.

容易验证这个 L/I 上的方括号运算是合理定义的. 如果 $a'+I=a+I$ 和 $b'+I=b+I$，则 $a-a'\in I$ 和 $b-b'\in I$，从而

$$[a',b']-[a,b]=[a',b']-[a',b]+[a',b]-[a,b]$$

776

$$= [a', b' - b] + [a' - a, b'] \in I.$$

例 9.169 （ⅰ）如果 $f: L \to L'$ 是李同态，则如通常那样定义它的核：

$$\ker f = \{a \in L : f(a) = 0\}.$$

易知 $\ker f$ 是 L 中的理想.

反之，由 $a \mapsto a + I$ 定义的**自然映射** $v: L \to L/I$ 是李同态，它的核是 I. 于是，L 的一个子空间是理想当且仅当它是某个李同态的核.

（ⅱ）如果 I 和 J 都是李代数 L 中的理想，则

$$IJ = \left\{ \sum_r [i_r, j_r] : i_r \in I, j_r \in J \right\}.$$

特别地，$L^2 = LL$ 是一个群的换位子群的李代数的类似：$L^2 = \{0\}$ 当且仅当 L 是阿贝尔的.

（ⅲ）对于李代数有群的导出列的类似. 李代数 L 的**导出列**是归纳定义的：

$$L^{(0)} = L; L^{(n+1)} = (L^{(n)})^2.$$

如果对一个李代数 L 存在某个 $n \geqslant 0$ 使得 $L^{(n)} = \{0\}$，则称 L 为**可解的**.

（ⅳ）对于李代数存在群的降中心列的类似. **降中心列**是归纳定义的：

$$L_1 = L; L_{n+1} = LL_n.$$

如果对一个李代数 L 存在某个 $n \geqslant 0$ 使得 $L_n = \{0\}$，则称 L 为**幂零的**. ■

在这个主题中，我们仅提出两个最先的定理. 如果 L 是李代数和 $a \in L$，则由 $\mathrm{ad}_a: x \mapsto [a, x]$ 给出的 $\mathrm{ad}_a: L \to L$ 是 L 上的线性变换（仅看作向量空间）. 如果 ad_a 是一个幂零算子；即有某个 $m \geqslant 1$ 使得 $(\mathrm{ad}_a)^m = 0$，则称 a 是 **ad-幂零的**.

定理（恩格尔定理） （ⅰ）如果 L 是任意域 k 上的有限维李代数，则 L 是幂零的当且仅当每个 $a \in L$ 都是 ad-幂零的.

（ⅱ）如果 L 是 $\mathfrak{gl}(n, k)$ 的子李代数，它的一切元素 A 都是幂零矩阵，则 L 可以表达为严格上三角的形式（一切对角线元素都是 0）；即对每个 $A \in L$ 存在非奇异矩阵 P 使得 PAP^{-1} 是严格上三角矩阵.

证明 见 Humphreys 所著的《Introduction to Lie Algebras and Representation Theory》，12 页.

777

■

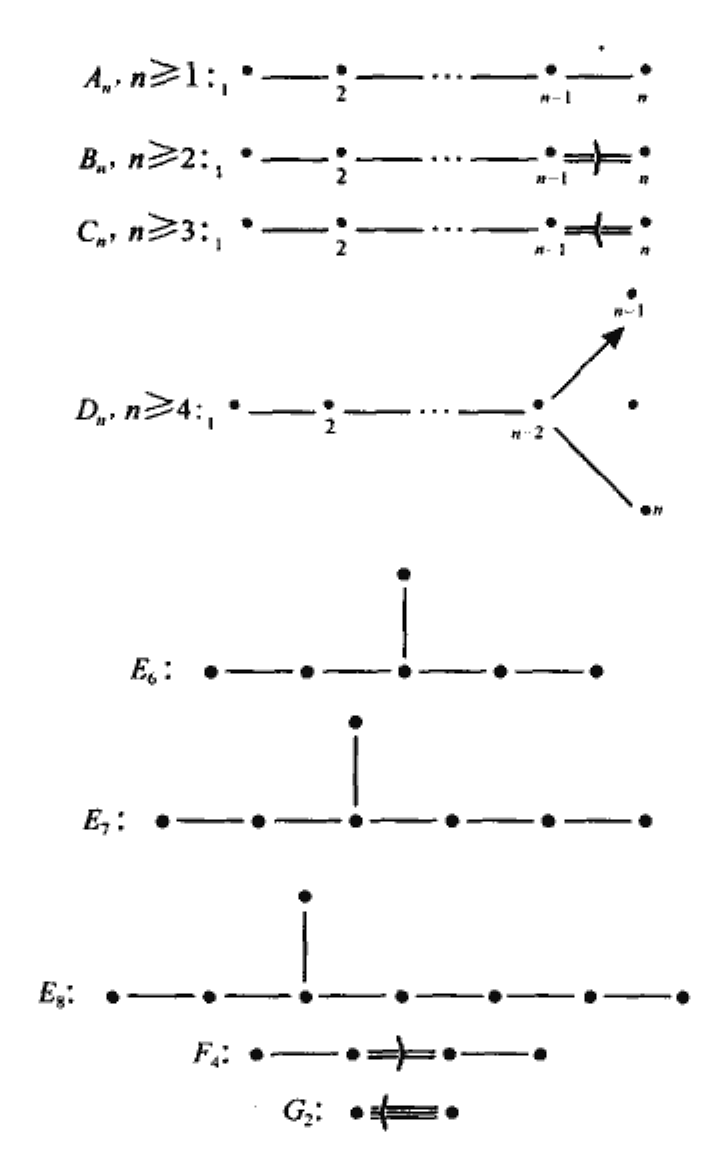
把恩格尔定理与习题 9.43（ⅰ）相比较，该习题是关于单幂零矩阵的简单情形. 因为有了恩格尔定理，所以有幂零李代数的名称；如同类似的有幂零群的名称. 系 5.48 说，每个有限 p-群可以作为子群嵌入 $\mathbb{F}_p$ 上的幺三角矩阵，它可以看作恩格尔定理的群论类似.

定理（李定理） $\mathfrak{gl}(n, k)$ 的每个可解子代数 L（其中 k 是一个代数闭域）都可以表达为（未必严格的）上三角形式；即对每个 $A \in L$，存在非奇异矩阵 P 使得 PAP^{-1} 是上三角的.

证明 见 Humphreys 所著的《Introduction to Lie Algebras and Representation Theory》，16 页.

■

李代数的进一步研究导出特征 0 的代数闭域上的属于嘉当和基灵的一切有限维单李代数的分类（最近，特征 p 中一切有限维单李代数的分类已经给出，其中 $p > 7$）. 他们把每个这种代数和某个叫做根系的几何结构相联系，根系由嘉当矩阵刻画. 而嘉当矩阵由邓肯图刻画.



778

每个邓肯图由C上的一个单李代数产生，两个这样的代数同构当且仅当它们有相同的邓肯图．读者可参考 Humphreys 所著的《Introduction to Lie Algebras and Representation Theory》第 4 章和 Jacobson 所著的《Lie Algebras》第 4 章．

还有其他重要的未必结合的代数．**若尔当代数**是交换代数 A，其中对一切 x，$y\in A$ 雅可比恒等式被

$$(x^2,y)x = x^2(yx)$$

替代．它们由若尔当引入，从而提供为量子力学设置的一个代数．若尔当代数的一个例子是特征不为 2 的域上一切 $n\times n$ 矩阵的一个子空间，配置以二元运算 $A*B$，其中

$$A*B=\frac{1}{2}(AB+BA).$$

未必结合代数的另一个来源是组合学．域 k 上射影平面 $P(k)$ 的通常构造作为 k^3 中一切过原点的直线族，它导出用“齐次坐标”$[x,y,z]$描述它的点，其中 $x,y,z\in k$. 定义一个抽象的**射影平面**为有序对$(X,\mathcal{L})$，其中 X 是一个有限集，$\mathcal{L}$是 X 的子集族，叫做直线，满足下列公理：

（ⅰ）一切直线有相同的点数；

（ⅱ）在 X 中给定两个点，有唯一的直线包含它们．

我们要引入齐次坐标来描述这种射影平面的点，但一开始并不给定域 k. 相反，我们考察 X 上一个函数的集团$\mathcal{K}$，叫做*直射变换*，并给$\mathcal{K}$配置两个二元运算（叫做加法和乘法）．一般来说，$\mathcal{K}$未必是一个结合代数，但有某种代数性质——乘法的交换性和结合性——对应于射影平面的几何性质——分别为帕普斯（Pappus）的一个定理和德萨格（Desargues）的一个定理．

一个重要的非结合代数是**凯莱数**（有时叫做八进制数），它是包含四元数作为子代数的八维实向量空间（见 Albert 所编的《Studies in Modern Algebra》中 Curtis 的论文）. 确实，在每个非零元素都有乘法逆的意义下，凯莱数形成一个实可除未必结合代数. 凯莱数得到额外的关注（比之其他未必结合代数）是因为它的自同构群具有有趣的性质. 例如，例外单李代数 E_8 同构于凯莱数的一切导子的李代数，而最大的零散有限单群是格里斯(R. Griess) 构造的某种非结合代数的自同构群.

779

习题

9.100 考虑 $n=2$ 时的德拉姆复形：

$$0 \to \Omega^0(X) \xrightarrow{d^0} \Omega^1(X) \xrightarrow{d^1} \Omega^2(X) \to 0.$$

证明：如果 $f(x,y) \in A(X) = \Omega^0(X)$，则

$$\mathrm{d}^0 f = \frac{\partial f}{\partial x}\mathrm{d}x + \frac{\partial f}{\partial y}\mathrm{d}y,$$

且如果 $P\mathrm{d}x + Q\mathrm{d}y$ 是 1 阶形式，则

$$\mathrm{d}^1(P\mathrm{d}x + Q\mathrm{d}y) = \left(\frac{\partial Q}{\partial x} - \frac{\partial P}{\partial y}\right)\mathrm{d}x \wedge \mathrm{d}y.$$

9.101 证明：如果 L 和 L' 都是非阿贝尔二维李代数，则 $L \cong L'$.

9.102 (i) 证明由

$$Z(L) = \{a \in L : [a,x] = 0, \text{对一切 } x \in L\}$$

定义的李代数 L 的中心是 L 中的一个阿贝尔理想.

(ii) 举出满足 $Z(L) = \{0\}$ 的一个李代数 L 的例子.

(iii) 如果 L 是幂零的且 $L \neq \{0\}$，证明 $Z(L) \neq \{0\}$.

9.103 证明：如果 L 是 n 维李代数，则 $Z(L)$ 的维数不可能是 $n-1$.（与习题 2.69 比较.）

9.104 在 $\mathbb{C}^3$ 上配置一个叉积（用与 $\mathbb{R}^3$ 上相同的叉积公式）. 证明

780

$$\mathbb{C}^3 \cong \mathfrak{sl}(2,\mathbb{C}).$$

第10章 同　调

10.1 引言

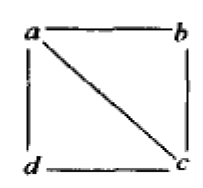
我做研究生的时候，同调代数不是一个普及的主题．一般认为它是一个怪诞的形式，学习它是令人厌烦的，学了它也没有多大用处．或许一个代数拓扑学者被迫去了解这个素材，但是确实没有别的人愿意在它上面浪费时间．少数忠实的信徒被看作数学边缘的工人，他们用精致的机器修补磨光这里那里粗糙的片断

当塞尔（J.-P. Serre）用同调代数刻画了正则局部环（它们是“有限整体维数”的交换诺特局部环）时，这个看法戏剧性地改变了，因为这使他能够证明一个正则局部环的任意局部化是正则的（之前只知道一些特殊情形）．同时，奥斯兰德（M. Auslander）和布赫斯包姆（D. A. Buchsbaum）完成了永田雅宜（M. Nagata）的工作，他们用整体维数证明每个正则局部环都是 UFD.

尽管新发现得到普及，但同调代数仍“不被重视”．例如，刚才提到的两个定理用了环的整体维数的概念，它是用模的同调维数来定义的．那时，卡普兰斯基开设了一门同调代数的课程．他的一个学生 S. Schanuel 注意到同一模的不同投射分解间存在着优美的关系（见命题 7.60）．卡普兰斯基（Kaplansky）抓住了这个今日称为 Schanuel 引理的结果，因为这使得他可以不必先发展同调代数的 Ext 和 Tor 的基本构造而定义一个模的同调维数，然后他能够证明塞尔定理和奥斯兰德-布赫斯包姆定理（卡普兰斯基对这门课程的叙述可以在他的书《Commutative Algebra》中找到）．然而，随着更多应用的发现和解决一些突出问题的同调和上同调理论的创立，同调代数的阻碍衰退了．今天，它是数学家的工具箱中另一个常用工具．

781

同调的基本思想来自格林（Green）定理，有洞的区域 R 上的二重积分等于 R 边界上的线积分．庞加莱（H. Poincaré）认识到对于一个拓扑空间 X，不同种类的洞可能意味着不同种类的连通性．为说明这一点，我们假定 X 能够“三角剖分”；即 X 可以分成有限个 n-单形，其中 $n\geqslant 0$：点是 0-单形，边是 1-单形，三角形是 2-单形，四面体是 3-单形，还有高维类似物．问题是 X 中“应该”成为某个 $(n+1)$-单形边界的 n-单形的并是否确实是这种边界．例如，当 $n=0$ 时，X 中的两个点 a 和 b 应该是 X 中一条道路的边界（端点）；如果 X 中存在一条道路连接一切点 a 和 b，则称 X 为*道路连通的*；如果没有这样的道路，则 X 有一个 0 维的洞．为举出一个有一维洞的例子，设 X 是*有孔平面*；即去掉原点的平面．一个三角形 Δ 的周长应该是一个 2-单形的边界，但如果 Δ 把原点包含在它的内部就不是这样；于是 X 有一维洞．如果 X 是平面抹去了包含原点的一个线段，或者甚至是抹去了包含原点的一个小圆盘，这个洞仍然是一维的；我们不考虑洞的大小，而是考虑可能的边界的大小．我们必须留意圆环而不是洞！



例如，在上面所画的矩形中，考虑有顶点 a,b,c 和边 $[a,b],[b,c],[a,c]$ 的三角形$[a,b,c]$. 它的边界$\partial[a,b,c]$应该是$[a,b]+[b,c]+[c,a]$. 但边是有向的（把 $[a,c]$ 想像为 a 到 c 的一条道路而 $[c,a]$ 是 c 到 a 的反方向的道路），因此写作 $[c,a]=-[a,c]$. 于是，边界是

$$\partial[a,b,c]=[a,b]-[a,c]+[b,c].$$

类似地，定义 $[a,b]$ 的边界为它的端点：

$$\partial[a,b]=b-a.$$

注意

$$\begin{aligned}\partial(\partial[a,b,c]) &= \partial([a,b]-[a,c]+[b,c])\\ &= b-a-(c-a)+c-b\\ &= 0.\end{aligned}$$

有顶点 a,b,c,d 的矩形是两个三角形 $[a,b,c]+[a,c,d]$ 的并，我们验证它的边界是 $\partial[a,b,c]+\partial[a,c,d]$（注意对角线 $[a,c]$ 出现两次，带有不同的符号，从而互相抵消）. 我们看到形式地把边界描述为带有符号的边或点的某种线性组合 u，则有 $\partial(u)=0$.

782

这个思想导出下面的构造. 对每个 $n\geqslant 0$，考虑 n-单形的一切形式线性组合；即组成以一切 n-单形为基的自由阿贝尔群$C_n(X)$，并称这种线性组合为 n-链. 一些 n-链应该是某些 $(n+1)$-单形的并的边界，把它们称为 n-圈（例如，把一个三角形的三条边加起来，附带合适选取的符号，是一个 1-圈）. 某些 n-链确实是边界，这种链称为 n-边界（如果 Δ 是有孔平面 X 上的三角形，原点不在它的内部，则 Δ 的边的交叉和是 1-边界；另一方面，如果原点在 Δ 的内部，则交叉和是 1-圈但不是 1-边界）. 一切 n-圈的族 $Z_n(X)$ 和一切 n-边界的族 $B_n(X)$ 都是 $C_n(X)$ 的子群. 同调群构造中的一个要素是子群 Z_n 和 B_n 可以用同态来定义：存在边界同态 $\partial_n:C_n(X)\to C_{n-1}(X)$ 使得 $Z_n=\ker\partial_n$和 $B_n=\operatorname{im}\partial_{n+1}$，从而存在阿贝尔群和同态的序列

$$\cdots\to C_3(X)\xrightarrow{\partial_3}C_2(X)\xrightarrow{\partial_2}C_1(X)\xrightarrow{\partial_1}C_0(X).$$

由此对一切 $n\geqslant 1$，$\partial_n\partial_{n+1}=0$，从而

$$B_n(X)\subseteq Z_n(X).$$

重要的群是商群 $Z_n(X)/B_n(X)$，记为 $H_n(X)$ 并称为 X 的 n 次同调⊖群. 在这个商群中残存的是 n-维洞；即不是 n-边界的那些 n-圈. 例如，$H_0(X)=0$ 意味 X 是道路连通的：如果存在没有由道路连通的两个点 a，$b\in X$，则 $a-b$ 为不是边界的一个圈，从而陪集 $a-b+B_0(X)$ 是 $H_0(X)$ 的非零元素. 对 $n\geqslant 1$，这些群能更精细地度量连通性类别. 拓扑学者用两种方法修改这个构造. 他们引入系数在阿贝尔群 G 中的同调，用 G 做链群序列的张量积，然后取同调群；他们也考虑系数在 G 中的上同调，运用反变函子 Hom(,G)到链群序列，然后取同调群. 同调代数因试图计算和找出空间的同调群之间的关系而产生.

783

⊖ 我未能找出这里使用的数学术语 Homology（同调）的词源. "homology" 来自 homo＋logos，它的意思是"对应". 它第一次作为数学术语使用是在 19 世纪初的射影几何中，作为特殊类型的直射变换的名称. 我找到的最早在圈和边界的意义下使用这个术语是在庞加莱的一篇论文中：Analysis Situs, Journal de l'École Polytechnique, Serise II, First issue, 1895（和 Oeuvres, vol. 5），但是他没有说明为什么选择这个术语. Emili Bifet 在私人通信中写道，"考虑由一个外部点的射影给出的两个不同的（超）平面之间的射影同调. 这个同调提出（并提供）用一种自然的方法把包含在一个平面中的单形的边界变形为在另一个中的对应单形的边界. 此外，它提出用一种自然的方法把一个边界变形为一个点. 这可能是庞加莱所想到的."

在命题 7.51 中，我们已经知道每个左 R-模 M，其中 R 是环，有一个用生成元和关系的描述．存在正合列

$$0 \longrightarrow \ker\varphi \xrightarrow{\iota} F \xrightarrow{\varphi} M \longrightarrow 0,$$

其中 F 是自由左 R-模，ι 是包含映射．如果 R 是 PID，则 $\ker\varphi$ 是自由的，这是因为自由模的每个子模本身也是自由的；如果 R 不是 PID，则 $\ker\varphi$ 可能不自由．现在取 $\ker\varphi$ 的生成元和关系：存在自由模 F_1 和正合列

$$0 \longrightarrow \ker\psi \xrightarrow{\kappa} F_1 \xrightarrow{\psi} \ker\varphi \longrightarrow 0.$$

如果定义 $F_1 \to F$ 为复合 $\iota\psi$，则存在第二个正合列

$$F_1 \xrightarrow{\iota\psi} F \xrightarrow{\varphi} M \longrightarrow 0.$$

迭代这个构造，存在一个长正合列

$$\cdots \to F_3 \to F_2 \to F_1 \to F \to M \to 0.$$

我们可以把子模 $\ker(F_n \to F_{n-1})$ 看作“关系上的关系”（19 世纪代数学家称这种高层关系为合系）．这个长正合列类似于拓扑中链群的序列．还有这种正合列存在的另外的背景；许多代数结构产生同调群的序列，从而可以把老定理翻译为同调语言．这种定理的例子是关于代数的希尔伯特定理 90（见系 10.129），关于李代数的怀特黑德引理（见雅各布森所著的《Lie Algebras》，77 页和 89 页）和关于群的定理 10.22，即舒尔-扎森豪斯引理．有方法计算同调和上同调群，这是同调代数对这个思想派系最重要的贡献．计算同调群最有效的方法是用*谱序列*，虽然没有它们也能够计算许多东西．我做研究生的时候，常想可以若无其事地说，“可用通常的谱序列论证”某某为真，但我从来没有这个勇气．[⊖]在本章的末尾，我们概要地说明什么是谱序列．

10.2 半直积

我们先研究群论中的基本问题．有正规子群 K 的群 G 可以“因子分解”为 K 和 G/K；扩张的研究涉及反过来的问题：从一个正规子群 K 和商群 $Q=G/K$ 可以获得 G 的多少信息？例如我们知道，如果 K 和 Q 都是有限的，则 $|G|=|K||Q|$．　[784]

非阿贝尔群序列的正合性，

$$\cdots \longrightarrow G_{n+1} \xrightarrow{d_{n+1}} G_n \xrightarrow{d_n} G_{n-1} \to \cdots,$$

如同对阿贝尔群的定义一样：对一切 $n, \mathrm{im}d_{n+1} = \ker d_n$. 当然，每个 $\ker d_n$ 是 G_n 的正规子群．

定义　*如果 K 和 Q 都是群，则 K 和 Q 的扩张是一个短正合列*

$$1 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1.$$

记号 K 提醒我们是核，记号 Q 提醒我们是商．

术语*扩张*还有另一种用法，（中间）群 G（不是短正合列）称为一个*扩张*，如果它包含正规子群 K_1 满足 $K_1 \cong K$ 和 $G/K_1 \cong Q$．和大多数人一样，我们在两种意义下使用这个术语．

例 10.1　（i）直积 $K\times Q$ 是 K 和 Q 的扩张；它也是 Q 和 K 的扩张．

（ii）S_3 和 I_6 都是 I_3 和 I_2 的扩张．另一方面，I_6 是 I_2 和 I_3 的扩张，但 S_3 不是，因为 S_3 不包含

⊖　这个引言改编自我写的一个评论，发表在 *Bulletin of the American Mathematical Society*，Vol. 33，pp. 473～475，1996，经美国数学会允许而引用．

2 阶正规子群． ■

我们刚才已经看到，对任意给定的群的有序对，总存在一个和另一个的扩张（它们的直积），但也许还有其他的扩张．**扩张问题**是对给定的群对 K 和 Q 的一切可能的扩张进行分类．

在第 5 章中，我们讨论了扩张问题和若尔当-赫尔德定理之间的关系．如果群 G 有合成列

$$G = K_0 \geqslant K_1 \geqslant K_2 \geqslant \cdots \geqslant K_{n-1} \geqslant K_n = \{1\}$$

和单因子群 $Q_1,\cdots,Q_n$，其中对一切 $i \geqslant 1, Q_i = K_{i-1}/K_i$，则可以从 $Q_n, Q_{n-1},\cdots,Q_1$ 通过解扩张问题 n 次得到G. 现在一切有限单群已经有了分类，因此，如果能够解扩张问题，就可以纵览一切单群．

先回忆群可以划分为子群的陪集．我们已经定义了群 G 的子群 K 的一个陪集代表系，它是从 K 的每个陪集[⊖] Kt 中恰取一个元素组成的 G 的子集 T.

定义 如果

$$1 \to K \to G \xrightarrow{p} Q \to 1$$

785 是一个扩张，则**提升**是指函数 $\ell: Q \to G$ 使得 $p\ell = 1_Q$，它不必是同态．

给定一个陪集代表系，可以构造一个提升．对每个 $x \in Q, p$ 的满射性提供$\ell(x) \in G$使得 $p\ell(x) = x$；于是，函数 $x \mapsto \ell(x)$ 是一个提升．反之，给定一个提升，我们断言 $\operatorname{im}\ell$ 是 K 的一个陪集代表系．如果 Kg 是一个陪集，则 $p(g) \in Q$，比如 $p(g) = x$. 则 $p(g\ell(x)^{-1}) = 1$，从而 $a = g\ell(x)^{-1} \in K$ 且 $Kg = K\ell(x)$. 于是，每个陪集在 $\ell(Q)$ 中有代表元．最后，我们需要证明 $\ell(Q)$ 不包含同一陪集中的两个元素．如果 $K\ell(x) = K\ell(y)$，则存在 $a \in K$ 使得 $a\ell(x) = \ell(y)$. 把 p 作用到这个等式上；因 $p(a) = 1$，有 $x = y$，从而 $\ell(x) = \ell(y)$．

在我们讨论的扩张中引出下面的群．

定义 回忆群 K 的一个自同构是一个同构 $K \to K$. **自同构群**（记为 $\operatorname{Aut}(K)$）是指 K 的以复合为运算的一切自同构组成的群．

当然，扩张是对任意群 K 定义的，但我们把注意力集中在 K 是阿贝尔群的特殊情形．如果 G 是 K 和 Q 的扩张，有可能因为把 G 写作乘性的而把它的子群 K 写成加性的而产生混淆．因此我们将约定下面的记号：即使 G 不是阿贝尔的，G 中的运算也将用加法记号．系 10.4 给出这个决定的主要原因.

命题 10.2 设

$$0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$$

是一个阿贝尔群 K 和群 Q 的扩张，并设 $\ell: Q \to G$ 是提升．

（ⅰ）对每个$x \in Q$，定义为

$$\theta_x: a \mapsto \ell(x) + a - \ell(x)$$

的共轭 $\theta_x: K \to K$ 不依赖于 x 的提升$\ell(x)$的选取．[为方便起见，我们假定了 i 是一个包含映射；这仅仅使得可以把 $i(a)$ 写作 a.]

（ⅱ）定义为 $x \mapsto \theta_x$ 的函数 $\theta: Q \to \operatorname{Aut}(K)$是一个同态．

证明 （ⅰ）现在我们证明 θ_x 不依赖于 x 的提升 $\ell(x)$ 的选取．假定 $\ell'(x) \in G$ 且 $p\ell'(x) =$

⊖ 我们使用了左陪集 tK，但在本章中，子群 K 是正规子群，此时，对一切 $t \in G$ 有 $tK = Kt$. 于是，用左陪集还是右陪集只是看怎样方便．

x. 存在 $b\in K$ 使得$\ell'(x)=\ell(x)+b$[因为 $-\ell(x)+\ell'(x)\in\ker p=\operatorname{im} i=K$]. 因为 K 是阿贝尔群，所以

$$\ell'(x)+a-\ell'(x)=\ell(x)+b+a-b-\ell(x)$$
$$=\ell(x)+a-\ell(x).$$

（ii）由于 $K\lhd G$，因此 $\theta_x(a)\in K$，从而每个 $\theta_x:K\to K$；因为共轭是自同构，所以 θ_x 也是 K 的自同构.

786

剩下要证明 $\theta:Q\to \operatorname{Aut}(K)$是同态．如果 $x,y\in Q$ 和 $a\in K$，则

$$\theta_x(\theta_y(a))=\theta_x(\ell(y)+a-\ell(y))=\ell(x)+\ell(y)+a-\ell(y)-\ell(x),$$

而

$$\theta_{xy}(a)=\ell(xy)+a-\ell(xy).$$

但 $\ell(x)+\ell(y)$和 $\ell(xy)$都是 xy 的提升，从而由（i）得到等式 $\theta_x\theta_y=\theta_{xy}$． ■

粗略地说，同态 θ 告诉我们 K “如何” 成为 G 中的正规子群，因为群的同构复制可以用不同方式作为 G 的正规子群．例如，设 K 是 3 阶循环群并设 $Q=\langle x\rangle$是2阶循环群．如果 $G=K\times Q$，则 G 是阿贝尔群且 K 位于 G 的中心．此时，对一切 $a\in K$ 有 $\ell(x)+a-\ell(x)=a$ 且 $\theta_x=1_K$．另一方面，如果 $G=S_3$，则 $K=A_3$，它不在中心；如果 $\ell(x)=(1\ 2)$，则 $(1\ 2)(1\ 2\ 3)(1\ 2)=(1\ 3\ 2)$，且 θ_x 不是 1_K.

同态 θ 的存在给 K 配置了一个标量乘法使 K 成为一个左$\mathbb{Z}Q$-模，其中$\mathbb{Z}Q$ 是群环，它的元素是一切 $\sum_{x\in Q}m_x x$，其中 $m_x\in\mathbb{Z}$.

命题 10.3 设 K 和 Q 是群且 K 是阿贝尔群，则同态 $\theta:Q\to\operatorname{Aut}(K)$使 K 成为一个$\mathbb{Z}Q$-模，如果其标量乘法对一切 $a\in K$ 和 $x\in Q$ 由

$$xa=\theta_x(a)$$

定义．反之，如果 K 是一个左$\mathbb{Z}Q$-模，则 $x\mapsto\theta_x$ 定义了一个同态 $\theta:Q\to\operatorname{Aut}(K)$，其中 $\theta_x:a\mapsto xa$.

证明 定义标量乘法如下．每个 $u\in\mathbb{Z}Q$ 有形如 $u=\sum_{x\in Q}m_x x$ 的唯一表达式，其中 $m_x\in\mathbb{Z}$ 且几乎一切 $m_x=0$；定义

$$\Big(\sum_x m_x x\Big)a=\sum_x m_x\theta_x(a)=\sum_x m_x(xa).$$

我们验证模公理．因 θ 是同态，$\theta(1)=1_K$，从而对一切 $a\in K,1a=\theta_1(a)$. $\theta_x\in\operatorname{Aut}(K)$蕴涵 $x(a+b)=xa+xb$，由此对一切 $u\in\mathbb{Z}Q$ 有 $u(a+b)=ua+ub$．类似地，容易验证对 $u,v\in\mathbb{Z}Q$ 有 $(u+v)a=ua+va$．最后，对一切 $x,y\in Q,(xy)a=x(ya)$ 由此 $(uv)a=u(va)$；但

$$(xy)a=\theta_{xy}(a)=\theta_x(\theta_y(a))=\theta_x(ya)=x(ya).$$

逆命题的证明也很简单． ■

787

系 10.4 如果

$$0\to K\xrightarrow{i}G\xrightarrow{p}Q\to 1$$

是阿贝尔群 K 和群 Q 的扩张，如果定义

$$xa=\ell(x)+a-\ell(x),$$

其中 $\ell:Q\to G$ 是提升，$x\in Q$ 和 $a\in K$，则 K 是一个左$\mathbb{Z}Q$-模；此外，标量乘法不依赖于提升 ℓ 的选取．

证明 命题 10.2 和命题 10.3. ■

从现在开始，我们把术语“左$\mathbb{Z}Q$-模”缩写为“Q-模”.

回忆左 R-模的一个短正合列

$$0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$$

分裂如果存在同态 $j: C \to B$ 使得 $pj = 1_C$；此时，中间模同构于直和 $A \oplus C$. 下面是对群的类似定义.

定义 对于群的一个扩张

$$0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1,$$

如果存在同态 $j: Q \to G$ 使得 $pj = 1_Q$，则称它为**分裂扩张**. 分裂扩张中的中间群 G 叫做 K 和 Q 的**半直积**. 注意，我们并没有假定核 K 是阿贝尔群.

于是，一个扩张分裂当且仅当存在提升 j，且这个提升也是一个同态. 我们将使用下面的记号：记 K 的元素为 $a, b, c, \cdots$，记 Q 的元素为 x，y，z，$\cdots$.

命题 10.5 设 G 是有正规子群 K 的加法群.

（i）如果 $0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$ 是分裂扩张，其中 $j: Q \to G$ 满足 $pj = 1_Q$，则 $i(K) \cap j(Q) = \{0\}$ 和 $i(K) + j(Q) = G$.

（ii）此时，每个 $g \in G$ 有唯一表达式 $g = i(a) + j(x)$，其中 $a \in K$ 和 $x \in Q$.

（iii）设 K 和 Q 都是群 G 的子群且 $K \lhd G$，则 G 是 K 和 Q 的半直积当且仅当 $K \cap Q = \{0\}$，$K + Q = G$，且每个 $g \in G$ 有唯一的表达式 $g = a + x$，其中 $a \in K$ 和 $x \in Q$.

证明 （i）如果 $g \in i(K) \cap j(Q)$，则有 $a \in K$ 和 $x \in Q$ 使得 $g = i(a) = j(x)$. 现在 $g = j(x)$ 蕴涵 $p(g) = pj(x) = x$，而 $g = i(a)$ 蕴涵 $p(g) = pi(a) = 0$. 所以，$x = 0$ 和 $g = j(x) = 0$.

如果 $g \in G$，则 $p(g) = pjp(g)$（因为 $pj = 1_Q$），因此 $g - (jp(g)) \in \ker p = \operatorname{im} i$；从而存在 $a \in K$ 使得 $g - (jp(g)) = i(a)$，所以 $g = i(a) + j(pg) \in i(K) + j(Q)$.

788

（ii）因为 $G = i(K) + j(Q)$，每个元素 $g \in G$ 有因子分解 $g = i(a) + j(pg)$. 为证明唯一性，假设 $i(a) + j(x) = i(b) + j(y)$，其中 $b \in K$ 和 $y \in Q$，则 $-i(b) + i(a) = j(y) - j(x) \in i(K) \cap j(Q) = \{0\}$，从而 $i(a) = i(b)$ 和 $j(x) = j(y)$.

（iii）必要性是（ii）中 i 和 j 都是包含映射的特殊情形. 反之，每个 $g \in G$ 有唯一的因子分解 $g = a + x$，其中 $a \in K$ 和 $x \in Q$；定义 $p: G \to Q$ 为 $p(ax) = x$. 容易验证 p 是满同态满足 $\ker p = K$. ■

所以叫做半直积是因为 K 和 Q 的直积 G 除满足 $KQ = G$ 和 $K \cap Q = \{1\}$ 之外，还要求子群 K 和 Q 都是正规的；这里只有一个子群必须是正规的.

定义 如果 $K \leqslant G$ 和 $C \leqslant G$ 满足 $C \cap K = \{1\}$ 且 $KC = G$，则称 C 为 K 的补.

在半直积 G 中，子群 K 是正规的；另一方面，命题 10.5 证明象 $j(Q)$ 是 K 的补，它可以不是正规的. 例如，如果 $G = S_3$ 和 $K = A_3 = \langle(1\ 2\ 3)\rangle$，我们可以取 $C = \langle\tau\rangle$，其中 τ 是 S_3 中的任一对换；这个例子也表明补未必唯一. 然而，K 的任意两个补是同构的，这是因为 K 的补同构于 G/K.

半直积的定义允许核 K 是非阿贝尔的，这种群是自然地产生的. 例如，对称群 S_n 是交错群 A_n 和 I_2 的半直积. 然而，为了保持假设的统一，在课文中（除了一些习题之外）我们假定 K 是阿贝尔的，即使这个假设不总是必需的.

例 10.6　（ⅰ）直积 $K\times Q$ 是 K 和 Q 的半直积（也是 Q 和 K 的半直积）.

（ⅱ）阿贝尔群 G 是半直积当且仅当它是直积（通常叫做直和），这是因为阿贝尔群的每个子群都是正规的.

（ⅲ）二面体群 D_{2n} 是I_n 和I_2 的半直积. 如果 $D_{2n}=\langle a,b\rangle$，其中 $a^n=1, b^2=1$ 和 $bab=a^{-1}$，则$\langle a\rangle$是有$\langle b\rangle$作为补的正规子群.

（ⅳ）每个弗罗贝尼乌斯群是它的弗罗贝尼乌斯核和它的弗罗贝尼乌斯补的半直积.

（ⅴ）设 $G=\mathbb{H}^{\times}$，即非零四元数的乘法群. 易知如果$\mathbb{R}^+$是正实数的乘法群，则由

$$N(a+bi+cj+dk)=a^2+b^2+c^2+d^2$$

给出的范数 $N: G\to\mathbb{R}^+$ 是同态. 有一个"极式分解" $h=rs$，其中 $r>0$ 和 $s\in\ker N$，且 G 是 $\ker N$ 和$\mathbb{R}^+$的半直积.（正规子群 $\ker N$ 是 3-球面.）在习题 10.4 中，我们会看到 $\ker N\cong SU(2,\mathbb{C})$，它是特殊酉群.

789

（ⅵ）阶为素数幂的循环群不是半直积，这是因为它们不可能是两个真子群的直和. ■

定义　*设 K 是 Q-模. 如果 K 和 Q 的一个扩张满足对一切 $x\in Q$ 和 $a\in K$ 有*

$$xa=\ell(x)+a-\ell(x);$$

*即给定的$\mathbb{Z}Q$在 K 上的标量乘法和系 10.4 中从共轭产生的标量乘法一致，则称 K 和 Q 的扩张***实现算子**.

下面是构造.

定义　*设 Q 是群并设 K 是 Q-模. 定义*

$$G=K\rtimes Q$$

为一切有序对 $(a,x)\in K\times Q$ 的集合具有运算

$$(a,x)+(b,y)=(a+xb,xy).$$

注意在 $K\rtimes Q$ 中 $(a,1)+(0,x)=(a,x)$.

命题 10.7　*给定群 Q 和 Q-模 K，则 $G=K\rtimes Q$ 是 K 和 Q 的实现算子的半直积.*

证明　我们先证明 G 是群. 关于结合性，

$$\begin{aligned}[(a,x)+(b,y)]+(c,z)&=(a+xb,xy)+(c,z)\\&=(a+xb+(xy)c,(xy)z).\end{aligned}$$

另一方面，

$$\begin{aligned}(a,x)+[(b,y)+(c,z)]&=(a,x)+(b+yc,yz)\\&=(a+x(b+yc),x(yz)).\end{aligned}$$

当然，由于 Q 中的结合性，$(xy)z=x(yz)$，第一个坐标也相等：因 K 是 Q-模，有

$$x(b+yc)=xb+x(yc)=xb+(xy)c.$$

于是，运算是结合的. G 的幺元是$(0,1)$，这是因为

$$(0,1)+(a,x)=(0+1a,1x)=(a,x),$$

(a,x)的逆是$(-x^{-1}a,x^{-1})$，这是因为

$$(-x^{-1}a,x^{-1})+(a,x)=(-x^{-1}a+x^{-1}a,x^{-1}x)=(0,1).$$

790

所以，根据习题 2.22，G 是群.

定义函数 $p: G\to Q$ 为 $p:(a,x)\mapsto x$. 因出现在第一个坐标中的元素只是一个"花招"，所以 p 是满同态且 $\ker p=\{(a,1): a\in K\}$. 如果定义 $i: K\to G$ 为 $i: a\mapsto(a,1)$，则

$$0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$$

是一个扩张．定义 $j: Q \to G$ 为 $j: x \mapsto (0,x)$．易知 j 是一个同态，这是因为 $(0,x)+(0,y)=(0,xy)$．现在 $pjx = p(0,x) = x$，从而 $pj = 1_Q$，于是扩张分裂；即 G 是 K 和 Q 的半直积．最后，G 实现算子：如果 $x \in Q$，则对某个 $b \in K$，x 的每个提升有 $\ell(x)=(b,x)$ 的形式，且

$$\begin{aligned}(b,x)+(a,1)-(b,x) &= (b+xa,x)+(-x^{-1}b,x^{-1})\\ &= (b+xa+x(-x^{-1}b),xx^{-1})\\ &= (b+xa-b,1)\\ &= (xa,1).\end{aligned}$$

■

我们暂时回到乘法记号．在下一证明中，读者将看到 $K \rtimes Q$ 中的运算来自恒等式

$$(ax)(by) = a(xbx^{-1})xy.$$

定理 10.8 设 K 是阿贝尔群．如果群 G 是 K 和一个群 Q 的半直积，则在 K 上存在一个 Q-模结构使得 $G \cong K \rtimes Q$.

证明 把 G 看作有正规子群 K 且 K 的补为 Q 的群．我们继续把 G 写作加性的（即使它可能不是阿贝尔的），从而把它的子群 Q 也写作加性的．如果 $a \in K$ 和 $x \in Q$，定义

$$xa = x+a-x;$$

即 xa 是 a 用 x 做成的共轭．根据命题 10.5，每个 $g \in G$ 有唯一的表达式 $g=a+x$，其中 $a \in K$ 和 $x \in Q$．由此，由 $\varphi: a+x \mapsto (a,x)$ 定义的 $\varphi: G \to K \rtimes Q$ 是双射．我们现在证明 φ 是同构．

$$\begin{aligned}\varphi((a+x)+(b+y)) &= \varphi(a+x+b+(-x+x)+y)\\ &= \varphi(a+(x+b-x)+x+y)\\ &= (a+xb,x+y).\end{aligned}$$

现在 $K \rtimes Q$ 中加法的定义给出

$$\begin{aligned}(a+xb,x+y) &= (a,x)+(b,y)\\ &= \varphi(a+x)+\varphi(b+y).\end{aligned}$$

791 我们现在用半直积构造一些群． ■

例 10.9 如果 $K=\langle a\rangle \cong \mathbb{I}_3$，则 K 的一个自同构完全由生成元 a 的象所确定；或者 $a \mapsto a$ 且自同构是 1_K，或者 $a \mapsto 2a$．所以，$\mathrm{Aut}(K) \cong \mathbb{I}_2$；我们记它的生成元为 φ，因此 $\varphi(a)=2a$ 和 $\varphi(2a)=a$；即 φ 是乘 2 的映射．设 $Q=\langle x\rangle \cong \mathbb{I}_4$，并定义 $\theta: Q \to \mathrm{Aut}(K)$ 为 $\theta_x = \varphi$；因此

$$xa = 2a \text{ 和 } x2a = a.$$

群

$$T = \mathbb{I}_3 \rtimes \mathbb{I}_4$$

是 12 阶群．如果定义 $s=(2a,x^2)$ 和 $t=(0,x)$，则读者可以验证

$$6s = 0 \text{ 和 } 2t = 3s = 2(s+t).$$

读者知道另外四个 12 阶群．基本定理说有两个 12 阶阿贝尔群：$\mathbb{I}_{12} \cong \mathbb{I}_3 \times \mathbb{I}_4$ 和 $\mathbb{I}_2 \times \mathbb{I}_6 \cong \mathbf{V} \times \mathbb{I}_3$．两个 12 阶非阿贝尔群是 A_4 和 $S_3 \times \mathbb{I}_2$（习题 10.7 要求读者证明 $A_4 \ncong S_3 \times \mathbb{I}_2$）．刚才构造的群 T 是一个新的例子，习题 10.17 说每个 12 阶群同构于这 5 个之一．[注意习题 2.85 (ii) 说 $D_{12} \cong S_3 \times \mathbb{I}_2$.] ■

例 10.10 设 p 是素数，并设 $K=\mathbb{I}_p \oplus \mathbb{I}_p$．因此，$K$ 是 $\mathbb{F}_p$ 上的向量空间，从而 $\mathrm{Aut}(K) \cong \mathrm{GL}(K)$．选取 K 的一组基 a，b，这给出同构 $\mathrm{Aut}(K) \cong \mathrm{GL}(2,p)$．设 $Q=\langle x\rangle$ 是 p 阶循环群．

定义 $\theta: Q \to \mathrm{GL}(2,p)$ 为对一切 $n \in \mathbb{Z}$，

$$\theta: x^n \mapsto \begin{bmatrix} 1 & 0 \\ n & 1 \end{bmatrix}.$$

于是，

$$xa = a + b \text{ 和 } xb = b.$$

容易验证换位子 $x + a - x - a = xa - a = b$，从而 $G = K \rtimes Q$ 是 p^3 阶群且 $G = \langle a, b, x \rangle$；这些生成元满足关系

$$pa = pb = px = 0, b = [x, a] \text{ 和} [b, a] = 0 = [b, x].$$

如果 p 是奇数，则根据命题 5.45 有 p^3 阶非阿贝尔群且指数为 p. 如果 $p = 2$，则 $|G| = 8$，习题 10.8 中要求读者证明 $G \cong D_8$，即 $D_8 \cong \mathbf{V} \rtimes \mathbb{I}_2$. 在例 10.6（ⅲ）中，我们看到 D_8 是$\mathbb{I}_4$ 和$\mathbb{I}_2$ 的半直积．于是，$\mathbf{V} \rtimes \mathbb{I}_2 \cong \mathbb{I}_4 \rtimes \mathbb{I}_2$，因此一个群可以有不同的半直积分解． ■

792

例 10.11 设 k 是域，并设 $k^{\times}$ 是它的乘法群．现在 $k^{\times}$ 由乘法作用在 k 上（如果 $a \in k$ 且 $a \neq 0$，则加性同态 $x \mapsto ax$ 是一个自同构，它的逆是 $x \mapsto a^{-1}x$）．所以，半直积 $k \rtimes k^{\times}$ 有定义．特别地，如果 $(b,a)(d,c) \in k \rtimes k^{\times}$，则

$$(b,a) + (d,c) = (ad + b, ac).$$

回忆一个仿射映射是形如 $f: x \mapsto ax + b$ 的一个函数 $f: k \to k$，其中 $a, b \in k$ 且 $a \neq 0$，一切仿射映射的集合在复合下是群 $\mathrm{Aff}(1,k)$. 注意，如果 $g(x) = cx + d$，则

$$\begin{aligned}(f \circ g)(x) &= f(cx + d) \\ &= a(cx + d) + b \\ &= (ac)x + (ad + b).\end{aligned}$$

现在易知函数 $\varphi: (b,a) \mapsto f$（其中 $f(x) = ax + b$）是同构 $k \rtimes k^{\times} \to \mathrm{Aff}(1,k)$． ■

习题

前三个习题中，群 K 不必是阿贝尔群；其他习题假定是阿贝尔群．

10.1 本题中的核可以不是阿贝尔群．

（ⅰ）证明 $\mathrm{SL}(2,\mathbb{F}_5)$是$\mathbb{I}_2$ 和 A_5 的扩张，但它不是一个半直积．

（ⅱ）如果 k 是域，证明 $\mathrm{GL}(n,k)$ 是 $\mathrm{SL}(n,k)$ 和 $k^{\times}$ 的半直积．

提示：一个补由一切矩阵 $\mathrm{diag}\{1,\cdots,1,a\}$ 组成，其中 $a \in k^{\times}$．

10.2 设 G 是 mn 阶群，其中 $(m,n) = 1$．证明一个 m 阶正规子群 K 在 G 中有补当且仅当存在 n 阶子群 $C \leqslant G$.（本题中的核可以不是阿贝尔群．）

10.3 （白尔）证明群 G 在一切群的范畴中是内射群[⊖]当且仅当 $G = \{1\}$．（本题中的核可以不是阿贝尔群.）

提示：设 A 是自由的并以$\{x,y\}$为基，并设 B 是半直积 $B = A \rtimes \langle z \rangle$，其中 z 是一个 2 阶元素，它由 $zxz = y$ 和 $zyz = x$ 作用在 A 上．

10.4 设 $SU(2)$ 是**特殊酉群**，它由一切行列式为 1 的满足下列性质的复数矩阵$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$组成：

$$a\bar{b} + c\bar{d} = 0, \quad a\bar{a} + b\bar{b} = 1, \quad c\bar{c} + d\bar{d} = 1.$$

⊖ 当白尔引入内射模的概念以证明这个结果的时候，术语 injective（内射）尚未创立．在认识了内射群是自由群的对偶之后，他开玩笑地称这种群为法西斯，并高兴地解释说这种群是平凡的．

如果 S 是例10.6(v)中$\mathbf{H}^{\times}$的子群，证明 $S\cong SU(2)$.

793

提示：用习题 8.2.

10.5 举出一个群的分裂扩张的例子

$$1 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1,$$

对于它不存在同态 $q: G \to K$ 使得 $qi = 1_K$．与习题 7.17 比较．

10.6 证明 $\mathbf{Q}$（即四元数群）不是半直积．

提示：回忆 $\mathbf{Q}$ 有唯一的 2 阶元素．

10.7 (i) 证明 $A_4 \not\cong S_3 \times \mathbb{I}_2$．

提示：用命题 2.64，该命题说 A_4 没有 6 阶子群．

(ii) 证明 12 阶非阿贝尔群：$A_4, S_3 \times \mathbb{I}_2$ 和 T 中的任两个都不同构．（见例 10.9.）

(iii) 仿射群 $\mathrm{Aff}(1, \mathbb{F}_4)$（见例 10.11）是一个 12 阶非阿贝尔群．它同构于 $A_4, S_3 \times \mathbb{I}_2$ 或 $T = \mathbb{I}_3 \rtimes \mathbb{I}_4$ 吗?

10.8 证明例 10.10 中构造的 8 阶群 G 和 D_8 同构．

10.9 如果 K 和 Q 都是可解群，证明 K 和 Q 的半直积也是可解群．

10.10 设 K 是阿贝尔群，设 Q 是群，并设 $\theta: Q \to \mathrm{Aut}(K)$ 是同态．证明 $K \rtimes Q \cong K \times Q$ 当且仅当 θ 是平凡映射（对一切 $x \in Q, \theta_x = 1_K$）．

10.11 (i) 如果 K 是阶为素数 p 的循环群，证明 $\mathrm{Aut}(K)$是 $p-1$ 阶循环群．

(ii) 设 G 是 pq 阶群，其中 $p>q$ 是素数．如果 $q \nmid (p-1)$，证明 G 是循环群．由此可知，比如说，每个 15 阶群是循环群．

10.12 设 G 是加法阿贝尔 p-群，其中 p 是素数．

(i) 如果 $(m,p)=1$，证明函数 $a \mapsto ma$ 是 G 的一个自同构．

(ii) 如果 p 是奇素数且 $G = \langle g \rangle$ 是 p^2 阶循环群，证明由 $\varphi: a \mapsto (sp+2)g$ 给出的 $\varphi: G \to G$ 是满足 $\varphi(pg) = 2pg$ 的唯一自同构．

10.3 一般扩张和上同调

现在我们研究一般扩张问题：给定群 Q 和阿贝尔群 K，求出 K 与 Q 的一切（不必分裂）扩张．根据我们对半直积的讨论，也就是对分裂扩张的讨论，把问题通过如下方式精练是合理的：假定 K 是 Q-模，然后寻找一切实现算子的扩张．

描述群 G 的一个方法是给出它的乘法表；即列出它的一切元素 $a_1, a_2, \cdots$ 和一切乘积 $a_i a_j$．事实上，我们构造半直积就是这样做的：元素是 $a \in K$ 和 $x \in Q$ 的一切有序对 (a,x)，乘法（其实是加法，因为我们选择把 G 写作加性的）是

$$(a,x)+(b,y) = (a+xb, xy).$$

1926 年，施赖埃尔用这种方法解决了扩张问题，本节呈示他的解．证明并不深奥，但涉及处理和组织一长列初等计算．

794

然而必须指出，施赖埃尔解并不能使我们确定不同构的中间群 G 的个数．当然，这个问题没有容易的答案．如果群 G 的阶为 n，则它的元素有 $n!$ 个不同的表，因此对于 G 有多达 $(n!)^n$ 个不同的乘法表（n 个行的每一行都有 $n!$ 种可能性）．现在假设 H 是另外一个 n 阶群．确定 G 和 H 是否同构本质上是比较它们的乘法表的族，以确定是否有 G 的一个乘法表和 H 的一个乘法表一致．

我们的策略是析取一个给定的扩张 G 的足够的性质，根据这些性质可以把 G 重构．于是，可以假定 K 是一个 Q-模，G 是 K 与 Q 的实现算子的扩张，且已选取了一个陪集代表系 $\ell: Q \to G$. 有了

这些初始根据，我们知道每个 $g \in G$ 有形如

$$g = a + \ell(x), a \in K \text{ 和 } x \in Q$$

的唯一的表达式；这是由于 G 是陪集 $K+\ell(x)$ 的不相交并．进一步，如果 $x,y \in Q$，则 $\ell(x)+\ell(y)$ 和 $\ell(xy)$ 是同一个陪集的代表元（没有说两个代表元相同!），因此存在元素 $f(x,y) \in K$ 使得

$$\ell(x) + \ell(y) = f(x,y) + \ell(xy).$$

定义 给定 K 与 Q 的扩张 G 的一个提升 $\ell: Q \to G$ 满足 $\ell(1)=0$，则一个**因子组**[㊀]（或余圈）是指函数 $f: Q\times Q \to K$ 满足对一切 x，$y\in Q$，

$$\ell(x) + \ell(y) = f(x,y) + \ell(xy).$$

选择提升满足 $\ell(1)=0$ 是自然的，因此把这个条件加入因子组的定义中；我们的因子组常叫做**正规化因子组**．

当然，因子组依赖于提升 ℓ 的选取．当 G 是分裂扩张时，存在构成同态的提升，相应的因子组恒等于 0. 因此，可以把因子组看作提升构成同态的障碍；即因子组描述一个扩张与分裂扩张有怎样的差异．

命题 10.12 设 Q 是群，K 是 Q-模，且 $0 \to K \to G \to Q \to 1$ 是一个实现算子的扩张．如果 $\ell: Q \to G$ 是满足 $\ell(1)=0$ 的提升，且 $f: Q\times Q \to K$ 是对应的因子组，则

(i) 对一切 $x,y \in Q$，

$$f(1,y) = 0 = f(x,1);$$

795

(ii) **余圈恒等式**成立：对一切 $x,y,z \in Q$，有

$$f(x,y) + f(xy,z) = xf(y,z) + f(x,yz).$$

证明 在定义 $f(x,y)$ 的等式

$$\ell(x) + \ell(y) = f(x,y) + \ell(xy)$$

中，令 $x=1$，可知 $\ell(y) = f(1,y) + \ell(y)$ [因根据我们新的假设，$\ell(1)=0$]，因此 $f(1,y)=0$．令 $y=1$ 可得 (i) 的另一个等式．

余圈恒等式来自 G 的结合性．对一切 $x,y,z \in Q$，有

$$\begin{aligned}[\ell(x)+\ell(y)]+\ell(z) &= f(x,y)+\ell(xy)+\ell(z)\\ &= f(x,y)+f(xy,z)+\ell(xyz).\end{aligned}$$

另一方面，

$$\begin{aligned}\ell(x)+[\ell(y)+\ell(z)] &= \ell(x)+f(y,z)+\ell(yz)\\ &= xf(y,z)+\ell(x)+\ell(yz)\\ &= xf(y,z)+f(x,yz)+\ell(xyz).\end{aligned}$$

■

更重要的是逆命题为真．下一个结果推广了命题 10.7 中 $K \rtimes Q$ 的构造．

定理 10.13 给定群 Q 和 Q-模 K，函数 $f: Q\times Q \to K$ 是因子组当且仅当它满足余圈恒等式[㊁]

$$xf(y,z) - f(xy,z) + f(x,yz) - f(x,y) = 0$$

和对一切 $x,y,z \in Q$ 有 $f(1,y) = 0 = f(x,1)$.

更精确地说，存在 K 与 Q 的实现算子的扩张，且存在陪集代表系 $\ell: Q \to G$，它对应的因子组为 f.

证明 必要性是命题 10.12. 关于逆命题，定义 G 为 $K\times Q$ 中一切有序对 (a,x) 的集合，配置运算

㊀ 如果转换为乘法记号，将看到因子组出现在因子分解 $\ell(x)\ell(y) = f(x,y)\ell(xy)$ 中．

㊁ 写作交错和的这个恒等式，使人联想到 10.1 节中描述的几何圈的公式．

$$(a,x)+(b,y)=(a+xb+f(x,y),xy).$$

（于是，如果 f 恒等于 0，则 $G=K\rtimes Q$.）G 是群的证明类似于命题 10.7 的证明．余圈恒等式用来证明结合性：

796

$$\begin{aligned}((a,x)+(b,y))+(c,z)&=(a+xb+f(x,y),xy)+(c,z)\\&=(a+xb+f(x,y)+xyc+f(xy,z),xyz)\end{aligned}$$

和

$$\begin{aligned}(a,x)+((b,y)+(c,z))&=(a,x)+(b+yc+f(y,z),yz)\\&=(a+xb+xyc+xf(y,z)+f(x,yz),xyz).\end{aligned}$$

余圈恒等式证明这些元素相等．

我们让读者证明幺元是 $(0,1)$ 且 (a,x) 的逆是

$$-(a,x)=(-x^{-1}a-x^{-1}f(x,x^{-1}),x^{-1}).$$

定义 $p:G\to Q$ 为 $p:(a,x)\mapsto x$. 因为第一个坐标中出现的只是一个“花招”，易知 p 是满同态且 $\ker p=\{(a,1):a\in K\}$. 如果定义 $i:K\to G$ 为 $i:a\mapsto(a,1)$，则有扩张 $0\to K\xrightarrow{i}G\xrightarrow{p}Q\to 1$.

为证明这个扩张实现算子，我们需要证明对每个提升 ℓ，关于一切 $a\in K$ 和 $x\in Q$ 有 $xa=\ell(x)+a-\ell(x)$. 现在有某个 $b\in K$ 使得 $\ell(x)=(b,x)$ 和

$$\begin{aligned}\ell(x)+(a,1)-\ell(x)&=(b,x)+(a,1)-(b,x)\\&=(b+xa,\ x)+(-x^{-1}b-x^{-1}f\ (x,\ x^{-1}),\ x^{-1})\\&=(b+xa+x\ [-x^{-1}b-x^{-1}f\ (x,\ x^{-1})]\ +f\ (x,\ x^{-1}),\ 1)\\&=(xa,\ 1).\end{aligned}$$

最后，需要证明 f 是由 ℓ 确定的因子组．选取提升为对一切 $x\in Q$，$\ell(x)=(0.x)$. 由 ℓ 确定的因子组 F 是由

$$\begin{aligned}F(x,y)&=\ell(x)+\ell(y)-\ell(xy)\\&=(0,x)+(0,y)-(0,xy)\\&=(f(x,y),xy)+(-(xy)^{-1}f(xy,(xy)^{-1}),(xy)^{-1})\\&=(f(x,y)+xy[-(xy)^{-1}f(xy,(xy)^{-1})]+f(xy,(xy)^{-1}),xy(xy)^{-1})\\&=(f(x,y),1)\end{aligned}$$

定义的． ■

下一个结果表明我们已经找到了 Q-模 K 与群 Q 的一切扩张．

定义 给定群 Q，Q-模 K 和因子组 f，令 $G(K,Q,f)$ 表示定理 10.13 中构造的 K 与 Q 的扩张的中间群．

定理 10.14 设 Q 是群，K 是 Q-模，并设 G 是 K 和 Q 的实现算子的扩张．则存在因子组 $f:Q\times Q\to K$ 使得

797

$$G\cong G(K,Q,f).$$

证明 设 $\ell:Q\to G$ 是提升，并设 $f:Q\times Q\to K$ 是对应的因子组；即对一切 x，$y\in Q$ 有

$$\ell(x)+\ell(y)=f(x,y)+\ell(xy).$$

因 G 是陪集的不相交并，$G=\bigcup_{x\in Q}K+\ell(x)$，每个 $g\in G$ 有唯一的表达式 $g=a+\ell(x)$，其中 $a\in K$ 和 $x\in Q$. 唯一性蕴涵由

$$\varphi : g = a + \ell(x) \mapsto (a, x)$$

给出的函数 $\varphi : G \to G(K, Q, f)$ 是合理定义的双射．现在证明 φ 是同构．

$$\begin{aligned}\varphi(a + \ell(x) + b + \ell(y)) &= \varphi(a + \ell(x) + b - \ell(x) + \ell(x) + \ell(y)) \\ &= \varphi(a + xb + \ell(x) + \ell(y)) \\ &= \varphi(a + xb + f(x,y) + \ell(xy)) \\ &= (a + xb + f(x,y), xy) \\ &= (a,x) + (b,y) \\ &= \varphi(a + \ell(x)) + \varphi(b + \ell(y)).\end{aligned}$$

■

注　为了后面的应用，注意，如果 $a \in K$，则 $\varphi(a) = \varphi(a + \ell(1)) = (a, 1)$，并且如果 $x \in Q$，则 $\varphi(\ell(x)) = (0, x)$．要是选取的提升 ℓ 满足 $\ell(1) \neq 0$，就没有这个结果．

现在我们已经用因子组描述了一切扩张，但因子组由提升确定．任一扩张都有许多不同的提升，因此依赖于提升选取的描述必有重复．

引理 10.15　给定群 Q 和 Q-模 K，设 G 是 K 和 Q 的实现算子的扩张．设 ℓ 和 ℓ' 是分别产生因子组 f 和 f' 的提升．则存在函数 $h : Q \to K$ 满足 $h(1) = 0$ 且对一切 $x, y \in Q$，

$$f'(x,y) - f(x,y) = xh(y) - h(xy) + h(x).$$

证明　对每个 $x \in Q$，$\ell(x)$ 和 $\ell'(x)$ 都位于 K 在 G 中的同一个陪集中，所以存在元素 $h(x) \in K$ 使得

$$\ell'(x) = h(x) + \ell(x).$$

因 $\ell(1) = 0 = \ell'(1)$，有 $h(1) = 0$. 主要公式导出如下：因为 G 实现算子，有

$$\begin{aligned}\ell'(x) + \ell'(y) &= [h(x) + \ell(x)] + [h(y) + \ell(y)] \\ &= h(x) + xh(y) + \ell(x) + \ell(y),\end{aligned}$$

798

继续有等式

$$\begin{aligned}\ell'(x) + \ell'(y) &= h(x) + xh(y) + f(x,y) + \ell(xy) \\ &= h(x) + xh(y) + f(x,y) - h(xy) + \ell'(xy).\end{aligned}$$

根据定义，f' 满足 $\ell'(x) + \ell'(y) = f'(x,y) + \ell'(xy)$. 所以，

$$f'(x,y) = h(x) + xh(y) + f(x,y) - h(xy).$$

因此，

$$f'(x,y) - f(x,y) = xh(y) - h(xy) + h(x).$$

■

定义　给定群 Q 和 Q-模 K，如果一个函数 $g : Q \times Q \to K$ 满足下列条件：存在函数 $h : Q \to K$ 满足 $h(1) = 0$ 使得对一切 $x, y \in Q$ 有

$$g(x,y) = xh(y) - h(xy) + h(x),$$

则称 g 是一个**上边缘**．

因为这个公式是一个交错和，它类似于 10.1 节中描述的关于几何边界的公式，所以产生上边缘这个术语．

我们刚才已经证明，如果 f 和 f' 是由不同提升形成的扩张 G 的因子组，则 $f' - f$ 是上边缘．

定义　给定群 Q 和 Q-模 K，定义

$$Z^2(Q,K) = \{\text{一切因子组 } f : Q \times Q \to K\},$$
$$B^2(Q,K) = \{\text{一切上边缘 } g : Q \times Q \to K\}.$$

命题 10.16 给定群 Q 和 Q-模 K，则 $Z^2(Q,K)$ 是一个阿贝尔群，它具有点态加法运算

$$f+f':(x,y)\mapsto f(x,y)+f'(x,y),$$

且 $B^2(Q,K)$ 是 $Z^2(Q,K)$ 的子群．

证明 为证明 Z^2 是群，只需证明 $f-f'$ 满足命题 10.12 中的两个恒等式．这是显然的：把关于 f 和 f' 的等式相减即可．

为证明 B^2 是 Z^2 的子群，我们需要证明每个上边缘 g 都是一个因子组；即 g 满足命题 10.12 中的两个恒等式．这也是简单的，留给读者．下一步需要证明 B^2 是非空子集；但零函数，即对一切 $x,y\in Q, g(x,y)=0$ 显然是一个上边缘．最后，我们证明 B^2 在减法下封闭．如果 $h,h':Q\to K$ 表明 g 和 g' 是上边缘，即 $g(x,y)=xh(y)-h(xy)+h(x)$ 和 $g'(x,y)=xh'(y)-h'(xy)+h'(x)$，则

799

$$(g-g')(x,y)=x(h-h')(y)-(h-h')(xy)+(h-h')(x). \qquad ■$$

一个给定的扩张有许多提升，因此有许多因子组，但这些因子组中任意两个的差是一个上边缘．因此提出下面的商群．

定义 定义**第二上同调群**为

$$H^2(Q,K)=Z^2(Q,K)/B^2(Q,K).$$

定义 给定群 Q 和 Q-模 K，如果对于 K 和 Q 的两个实现算子的扩张 G 和 G'，存在 G 的一个因子组 f 和 G' 的一个因子组 f' 使得 $f'-f$ 是上边缘，则称两个扩张 G 和 G' **等价**．

命题 10.17 给定群 Q 和 Q-模 K，K 和 Q 的两个实现算子的扩张 G 和 G' 等价当且仅当存在同构 $\gamma: G\to G'$ 使得下图交换：

$$\begin{array}{ccccccccc}
0 & \to & K & \xrightarrow{i} & G & \xrightarrow{p} & Q & \to & 1\\
 & & \downarrow{\scriptstyle 1_K} & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle 1_Q} & & \\
0 & \to & K & \xrightarrow{i'} & G' & \xrightarrow{p'} & Q & \to & 1
\end{array}$$

注 用图上追踪法可证明使得图交换的任一同态 γ 必是一个同构．

证明 假定两个扩张等价．我们先设置记号．设 $\ell: Q\to G$ 和 $\ell': Q\to G'$ 都是提升，设 f，f' 是对应的因子组；即对一切 $x,y\in Q$，有

$$\ell(x)+\ell(y)=f(x,y)+\ell(xy),$$

以及关于 f' 和 ℓ' 有类似的等式．等价意味着存在函数 $h: Q\to K$ 使得 $h(1)=0$ 以及对一切 $x,y\in Q$，

$$f(x,y)-f'(x,y)=xh(y)-h(xy)+h(x).$$

因 $G=\bigcup\limits_{x\in Q}K+\ell(x)$ 是不相交并，每个 $g\in G$ 有唯一的表达式 $g=a+\ell(x)$，其中 $a\in K$ 和 $x\in Q$；类似地，每个 $g'\in G'$ 有唯一的表达式 $g'=a+\ell'(x)$．

下面这部分的证明是定理 10.14 证明的推广．定义 $\gamma: G\to G'$ 为

$$\gamma(a+\ell(x))=a+h(x)+\ell'(x).$$

该函数使得图交换．如果 $a\in K$，则

800

$$\gamma(a)=\gamma(a+\ell(1))=a+h(1)+\ell'(1)=a;$$

进一步，

$$p'\gamma(a+\ell(x))=p'(a+h(x)+\ell'(x))=x=p(a+\ell(x)).$$

最后，γ 是同态：

$$\begin{aligned}\gamma([a+\ell(x)]+[b+\ell(y)])&=\gamma(a+xb+f(x,y)+\ell(xy))\\&=a+xb+f(x,y)+h(xy)+\ell'(xy),\end{aligned}$$

而

$$\begin{aligned}\gamma(a+\ell(x))+\gamma(b+\ell(y)) &= (a+h(x)+\ell'(x))+(b+h(y)+\ell'(y)) \\ &= a+h(x)+xb+xh(y)+f'(x,y)+\ell'(xy) \\ &= a+xb+(h(x)+xh(y)+f'(x,y))+\ell'(xy) \\ &= a+xb+f(x,y)+h(xy)+\ell'(xy).\end{aligned}$$

我们用了对 $f-f'$ 给出的等式 [记住除 $\ell'(xy)$ 以外的一切项都在阿贝尔群 K 中，因此它们可以重新排列].

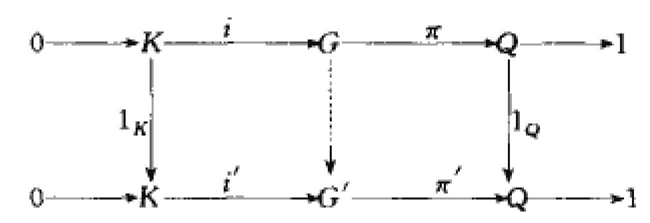
反之，假定存在同构 γ 使得图交换，从而对一切 $a\in K$，$\gamma(a)=a$ 且对一切 $x\in Q$,

$$x=p(\ell(x))=p'\gamma(\ell(x)),$$

由此 $\gamma\ell:Q\to G'$ 是提升．把 γ 作用到定义因子组 f 的等式 $\ell(x)+\ell(y)=f(x,y)+\ell(xy)$ 上，可知 γf 是由提升 $\gamma\ell$ 确定的因子组．但对一切 $x,y\in Q$，因为 $f(x,y)\in K$，因此有 $\gamma f(x,y)=f(x,y)$．所以，f 也是第二个扩张的因子组．另一方面，如果 f' 是第二个扩张的其他因子组，则定理 10.17 表明 $f-f'\in B^2$；即两个扩张等价． ■

我们说命题 10.17 中的同构 γ **实现**了等价．定理 10.14 后面的注表明同构 $\gamma:G\to G(K,Q,f)$ 实现了扩张的等价．

例 10.18　如果 K 与 Q 的两个实现算子的扩张等价，则它们的中间群同构．然而，逆命题不成立：我们举例说明两个不等价的扩张可以有同构的中间群．设 p 是奇素数，考虑下面的图：



定义 $K=\langle a\rangle$，它是 p 阶循环群，$G=\langle g\rangle=G'$，它是 p^2 阶循环群，$Q=\langle x\rangle$，其中 $x=g+K$．在最上面一行中，定义 $i(a)=pg$ 和 π 为自然映射；在底下一行中，定义 $i'(a)=2pg$ 和 π' 为自然映射．注意，因为 p 是奇数，所以 i' 是单射． 801

假设存在同构 $\gamma:G\to G'$ 使得图交换．第一个方块的交换性蕴涵 $\gamma(pa)=2pa$，根据习题 10.12 (ii)，这迫使 $\gamma(g)=2g$；第二个方块的交换性给出 $g+K=2g+K$；即 $g\in K$．由此可知两个扩张不等价． ■

下一个定理总结了本节中的计算．

定理 10.19 (施赖埃尔)　设 Q 是群，K 是 Q-模，并设 $e(Q,K)$ 表示 K 和 Q 的实现算子的扩张的一切等价类的族．存在双射

$$\varphi: H^2(Q,K)\to e(Q,K),$$

它对于分裂扩张类取 0.

证明　记扩张

$$0\to K\to G\to Q\to 1$$

的等价类为 $[G]$．定义 $\varphi: H^2(Q,K)\to e(Q,K)$ 为

$$\varphi: f+B^2\mapsto[G(K,Q,f)],$$

其中 f 是扩张的因子组，目标扩张如定理 10.13 所述构造．

首先，φ 是合理定义的单射：根据命题 10.17，f 和 g 是因子组满足 $f+B^2=g+B^2$ 当且仅当

$[G(K,Q,f)] = [G(K,Q,g)]$. 为证明 φ 是满射，设 $[G] \in e(Q,K)$. 根据定理 10.14 和它后面的注，有某个因子组 f 使得 $[G] = [G(K,Q,f)]$，从而 $[G] = \varphi(f + B^2)$. 最后，零因子组对应半直积. ■

如果 H 是群，且存在双射 $\varphi: H \to X$，其中 X 是集合，则存在定义在 X 上的唯一运算使 X 成为一个群且 φ 是同构：给定 $x,y \in X$，有 $g,h \in H$ 使得 $x = \varphi(g)$ 和 $y = \varphi(h)$，我们定义 $xy = \varphi(gh)$. 特别地，有一个方法把扩张的两个等价类相加；这个方法叫做**白尔和**（见 10.6 节）.

系 10.20 如果 Q 是群，K 是 Q-模，且 $H^2(Q,K) = \{0\}$，则 K 和 Q 的每个实现算子的扩张都是一个半直积.

证明 根据定理，$e(Q,K)$ 只有一个元素；因分裂扩张恒存在，这一元素必是分裂扩张的等价类. 所以，K 和 Q 的每个实现算子的扩张分裂，从而它的中间群是半直积. ■

802

我们现在来应用施赖埃尔定理.

定理 10.21 设 G 是 mn 阶有限群，其中 $(m,n)=1$. 如果 K 是 m 阶阿贝尔正规子群，则 K 有补且 G 是半直积.

证明 定义 $Q = G/K$. 根据系 10.20，只要证明每个因子组 $f: Q \times Q \to K$ 是一个上边缘. 定义 $\sigma: Q \to K$ 为

$$\sigma(x) = \sum_{y \in Q} f(x,y);$$

因为 Q 是有限的而 K 是阿贝尔的，所以 σ 是合理定义的. 现在取余圈恒等式

$$xf(y,z) - f(xy,z) + f(x,yz) - f(x,y) = 0$$

在一切 $z \in Q$ 上的和，得

$$x\sigma(y) - \sigma(xy) + \sigma(x) = nf(x,y)$$

(因 z 遍历 Q，所以 yz 也遍历 Q). 因 $(m,n) = 1$，存在整数 s 和 t 使得 $sm + tn = 1$. 定义 $h: Q \to K$ 为

$$h(x) = t\sigma(x).$$

注意 $h(1) = 0$ 和

$$xh(y) - h(xy) + h(x) = f(x,y) - msf(x,y).$$

但 $sf(x,y) \in K$，从而 $msf(x,y) = 0$. 所以，f 是上边缘. ■

注 霍尔证明，如果 G 是 mn 阶有限可解群，其中 $(m,n) = 1$，则 G 有 m 阶子群且任何两个这样的子群共轭. 特别地，在可解群中，每个（不必正规）西罗子群都有补. 由于这个定理，对于有限群 G 的一个（不必正规）子群 H，如果 $(|H|,[G:H]) = 1$，则称 H 为**霍尔子群**. 于是，定理 10.21 常陈述为任意有限群的每个正规霍尔子群都有补.

我们现在用一点群论来去掉 K 是阿贝尔群的假设.

定理 10.22（舒尔-扎森豪斯[⊖]引理） 设 G 是 mn 阶有限群，其中 $(m,n) = 1$. 如果 K 是 m 阶正规子群，则 K 有补且 G 是半直积.

803

证明 根据习题 10.2，只要证明 G 包含一个 n 阶子群；我们对 $m \geq 1$ 用归纳法证明这种子群的存在性. 当然，基础步 $m=1$ 为真.

假设存在 K 的真子群 T 满足 $\{1\} < T \lhd G$，则 $K/T \lhd G/T$ 和 $(G/T)/(K/T) \cong G/K$ 的阶为 n. 因

⊖ 1904 年，舒尔对 Q 是循环群的特殊情形证明了这个定理. 1938 年，扎森豪斯对任意有限群 Q 证明了这个定理.

$T < K$，有 $|K/T| < |K| = m$，从而归纳假设提供子群 $N/T \leqslant G/T$ 使得 $|N/T| = n$. 现在 $|N| = n|T|$，其中 $(|T|, n) = 1$［因为 $|T|$ 是 $|K| = m$ 的因数］，因此 T 是 N 的正规子群，它的阶与指数互素．因 $|T| < |K| = m$，归纳假设提供了 N 的 n 阶子群 C（显然它是 G 的子群）．

现在可以假定 K 是 G 的极小正规子群；即没有 G 的正规子群 T 满足 $\{1\} < T < K$．设 p 是 $|K|$ 的素因数，并设 p 是 K 的西罗 p-子群．根据费拉蒂尼命题，即习题 5.21，有 $G = KN_G(P)$. 所以，

$$\begin{aligned} G/K &= KN_G(P)/K \\ &\cong N_G(P)/(K \cap N_G(P)) \\ &= N_G(P)/N_K(P). \end{aligned}$$

因此，$|N_K(P)|n = |N_K(P)||G/K| = |N_G(P)|$．如果 $N_G(P)$ 是 G 的真子群，则 $|N_K(P)| < m$，且归纳假设提供 $N_G(P) \leqslant G$ 的 n 阶子群．所以可以假定 $N_G(P) = G$；即 $P \lhd G$.

因 $\{1\} < P \leqslant K$ 和 P 是 G 中的正规子群，而 K 是极小正规子群，因此必有 $P = K$．但 P 是一个 p-群，因此它的中心 $Z(P)$ 是非平凡的．根据习题5.19(v)，有 $Z(P) \lhd G$，并且因为 $P = K$ 是 G 的极小正规子群，所以 $Z(P) = P$．由此，P 是阿贝尔的，问题简化成定理 10.21. ■

系 10.23 *如果有限群 G 有正规西罗 p-子群 P，其中 P 是 $|G|$ 的某个素因数，则 G 是半直积；精确地说，P 有补．*

证明 西罗子群的阶和指数是互素的． ■

舒尔-扎森豪斯引理还有另一半未曾叙述：如果 K 是 G 的正规子群，它的阶和指数互素，则 K 的任两个补是共轭子群．我们现在证明存在 $H^2(K,Q)$ 的类似物，当 K 是阿贝尔群时，它的消失蕴涵补的共轭．群 $H^1(K,Q)$ 和 $H^2(K,Q)$ 一样，由初等计算的序列形成．

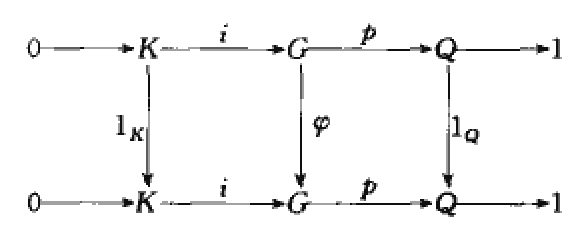
我们先从一个计算结果开始．设 Q 是群，K 是 Q-模，并设 $0 \to K \to G \to Q \to 1$ 是分裂扩张．选取提升 $\ell: Q \to G$，从而每个元素 $g \in G$ 有形如

$$g = a + \ell x$$

的唯一的表达式，其中 $a \in K$ 和 $x \in Q$.

804

定义 *称群 G 的一个自同构 φ **稳定**一个扩张 $0 \to K \to G \to Q \to 1$，如果下图交换：*



K 和 Q 的一个扩张的一切稳定化自同构的集合，其中 K 是 Q-模，在复合下形成一个群，记为

$$\mathrm{Stab}(Q,K).$$

注意一个稳定化自同构是实现一个扩张和它自己等价的同构．在命题 10.26 中将看到 $\mathrm{Stab}(Q,K)$ 不依赖于扩张．

命题 10.24 *设 Q 是群，K 是 Q-模，并设*

$$0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$$

是分裂扩张．如果 $\ell: Q \to G$ 是提升，则形如

$$\varphi(a + \ell x) = a + d(x) + \ell x$$

（其中 $d(x) \in K$）的每个稳定化自同构 $\varphi: G \to G$ 不依赖于提升 ℓ 的选取．此外，这个公式定义了一

个稳定化自同构当且仅当对一切 $x,y\in Q$，函数 $d:Q\to K$ 满足

$$d(xy)=d(x)+xd(y).$$

证明 如果 φ 是稳定化自同构，则 $\varphi i=i$，其中 $i:K\to Q$，且 $p\varphi=p$. 因为假定 i 是包含映射[这仅仅使我们可以方便地把 $i(a)$ 写作 a]，对一切 $a\in K$ 有 $\varphi(a)=a$. 为了运用 φ 的第二个约束，假设有某个 $d(x)\in K$ 和 $y\in Q$ 使得 $\varphi(\ell x)=d(x)+\ell y$. 则

$$\begin{aligned} x &= p(\ell x)\\ &= p\varphi(\ell x)\\ &= p(d(x)+\ell y)\\ &= y; \end{aligned}$$

即 $x=y$. 所以，

805

$$\varphi(a+\ell x)=\varphi(a)+\varphi(\ell x)=a+d(x)+\ell x.$$

为证明公式对于 d 成立，我们先证明 d 不依赖于提升的选取. 假设 $\ell':Q\to G$ 是另一个提升，因此有某个 $d'(x)\in K$ 使得 $\varphi(\ell' x)=d'(x)+\ell' x$. 现在因为 $p\ell' x=x=p\ell x$，存在 $k(x)\in K$ 使得 $\ell' x=k(x)+\ell x$. 所以，

$$\begin{aligned} d'(x) &= \varphi(\ell' x)-\ell' x\\ &= \varphi(k(x)+\ell x)-\ell' x\\ &= k(x)+d(x)+\ell x-\ell' x\\ &= d(x), \end{aligned}$$

这是因为 $k(x)+\ell x-\ell' x=0$.

因 $d(x)$ 不依赖于提升 ℓ 的选取，又因扩张分裂，我们可以假定 ℓ 是同态：$\ell x+\ell y=\ell(xy)$. 用两种方法计算 $\varphi(\ell x+\ell y)$. 一方面，

$$\varphi(\ell x+\ell y)=\varphi(\ell(xy))=d(xy)+\ell(xy).$$

另一方面，

$$\begin{aligned} \varphi(\ell x+\ell y) &= \varphi(\ell x)+\varphi(\ell y)\\ &= d(x)+\ell x+d(y)+\ell y\\ &= d(x)+xd(y)+\ell(xy). \end{aligned}$$

对于逆命题的证明，如果 $\varphi(a+\ell x)=a+d(x)+\ell x$，其中 d 满足给定的恒等式，则容易证明 φ 是稳定化同构，把它留给读者.

给 d 这样的函数一个名称. ■

定义 设 Q 是群，并设 K 是 Q-模. 一个**导子**[⊖]（或**交叉同态**）是指函数 $d:Q\to K$ 满足

$$d(xy)=xd(y)+d(x).$$

一切导子的集合 $\mathrm{Der}(Q,K)$ 在点态加法下是一个阿贝尔群[如果 K 是平凡 Q-模，则 $\mathrm{Der}(Q,K)=\mathrm{Hom}(Q,K)$].

如果 d 是导子，则 $d(11)=1d(1)+d(1)\in K$，从而 $d(1)=0$.

⊖ 早先我们定义（不必结合的）环 R 的导子为函数 $d:R\to R$ 满足 $d(xy)=d(x)y+xd(y)$. 这里的导子是在模上定义的，而不是环.

例 10.25　（ⅰ）如果 Q 是群和 K 是 Q-模，则形如 $u(x)=xa_0-a_0$（其中 $a_0\in K$）的函数 $u:Q\to K$ 是一个导子：

$$\begin{aligned}u(x)+xu(y)&=xa_0-a_0+x(ya_0-a_0)\\&=xa_0-a_0+xya_0-xa_0\\&=xya_0-a_0\\&=u(xy).\end{aligned}$$

806

形如 $u(x)=xa_0-a_0$ 的导子 u 叫做**主导子**.

如果 Q 在 K 上的作用是共轭，$xa=x+a-x$，则

$$xa_0-a_0=x+a_0-x-a_0;$$

即 xa_0-a_0 是 x 和 a_0 的换位子.

（ⅱ）容易验证一切主导子的集合 $\mathrm{PDer}(Q,K)$ 是 $\mathrm{Der}(Q,K)$ 的子群. ■

回忆 $\mathrm{Stab}(Q,K)$ 表示 K 和 Q 的一个扩张的一切稳定化自同构的群.

命题 10.26　*如果 Q 是群，K 是 Q-模，$0\to K\to G\to Q\to 1$ 是一个分裂扩张，则存在同构 $\mathrm{Stab}(Q,K)\to\mathrm{Der}(Q,K)$.*

证明　设 φ 是稳定化自同构. 如果 $\ell:Q\to G$ 是提升，则命题 10.24 说 $\varphi(a+\ell x)=a+d(x)+\ell x$，其中 d 是导子. 因这个命题进一步说 d 不依赖于提升的选取，所以 $\varphi\mapsto d$ 是合理定义的函数 $\mathrm{Stab}(Q,K)\to\mathrm{Der}(Q,K)$，易知它是一个同态.

为证明这个映射是同构，我们构造它的逆. 如果 $d\in\mathrm{Der}(Q,K)$，定义 $\varphi:G\to G$ 为 $\varphi(a+\ell x)=a+d(x)+\ell x$. 现在根据命题 10.24，$\varphi$ 是稳定化的，且 $d\mapsto\varphi$ 是所要的逆函数. ■

从 $\mathrm{Stab}(Q,K)$ 的定义并不能明显地看出它是阿贝尔群，这是因为它的二元运算是复合. 然而，因为 $\mathrm{Der}(Q,K)$ 是阿贝尔群，所以 $\mathrm{Stab}(Q,K)$ 也是阿贝尔群.

回忆如果群 G 的一个自同构 φ 是共轭，则称 φ 为*自内同构*；即存在 $c\in G$ 使得对一切 $g\in G$ 有 $\varphi(g)=c+g-c$（如果 G 写作加性的）.

引理 10.27　*设 $0\to K\to G\to Q\to 1$ 是分裂扩张，并设 $\ell:Q\to G$ 是提升. 则函数 $\varphi:G\to G$ 是关于某个 $a_0\in K$ 的稳定化内自同构当且仅当*

$$\varphi(a+\ell x)=a+xa_0-a_0+\ell x.$$

证明　如果记 $d(x)=xa_0-a_0$，则 $\varphi(a+\ell x)=a+d(x)+\ell x$. 但 d 是一个（主）导子，因此根据命题 10.24，φ 是稳定化自同构. 最后，φ 是由 $-a_0$ 形成的共轭，这是因为

$$-a_0+(a+\ell x)+a_0=-a_0+a+xa_0+\ell x=\varphi(a+\ell x).$$

反之，假定 φ 是稳定化共轭. φ 是稳定化的就是说 $\varphi(a+\ell x)=a+d(x)+\ell x$；$\varphi$ 是由 $a_0\in K$ 形成的共轭就是说 $\varphi(a+\ell x)=a_0+a+\ell x-a_0$. 但 $a_0+a+\ell x-a_0=a_0+a-xa_0+\ell x$，因此正如所要的 $d(x)=a_0-xa_0$. ■

807

定义　*如果 Q 是群和 K 是 Q-模，定义*

$$H^1(Q,K)=\mathrm{Der}(Q,K)/\mathrm{PDer}(Q,K),$$

其中 $\mathrm{PDer}(Q,K)$ 是由一切主导子组成的 $\mathrm{Der}(Q,K)$ 的子群.

命题 10.28　*设 $0\to K\to G\to Q\to 1$ 是分裂扩张，并设 C 和 C' 是 K 在 G 中的补. 如果 $H^1(Q,$*

$K) = \{0\}$，则 C 和 C' 共轭．

证明 因 G 是半直积，存在以 C 为象的提升 $\ell: Q \to G$ 和以 C' 为象的提升 $\ell': Q \to G$，且它们都是同态．于是，分别由这两个提升确定的因子组 f 和 f' 都恒等于零，因此 $f' - f = 0$．但引理 10.15 说存在 $h: Q \to K$，即 $h(x) = \ell' x - \ell x$，使得

$$0 = f'(x,y) - f(x,y) = xh(y) - h(xy) + h(x);$$

于是，h 是导子．因 $H^1(Q,K) = \{0\}$，所以 h 是主导子：存在 $a_0 \in K$ 使得对一切 $x \in Q$ 有

$$\ell' x - \ell x = h(x) = xa_0 - a_0.$$

因 G 中的加法满足 $\ell' x - a_0 = -xa_0 + \ell' x$，所以有

$$\ell x = a_0 - xa_0 + \ell' x = a_0 + \ell' x - a_0.$$

但 $\mathrm{im}\ell = C$ 和 $\mathrm{im}\ell' = C'$，因此 C 和 C' 经 a_0 共轭． ■

我们现在可以补充舒尔-扎森豪斯定理．

定理 10.29 设 G 是 mn 阶有限群，其中 $(m,n) = 1$．如果 K 是 m 阶阿贝尔正规子群，则 G 是 K 和 G/K 的半直积，且 K 的任两个补共轭．

证明 根据命题 10.28，只要证明 $H^1(Q,K) = \{0\}$，其中 $Q = G/K$．首先注意 $|Q| = |G|/|K| = mn/m = n$．

设 $d: Q \to K$ 是导子：对一切 $x, y \in Q$，有

$$d(xy) = xd(y) + d(x).$$

这个等式对一切 $y \in Q$ 取和得

$$\Delta = x\Delta + nd(x),$$

其中 $\Delta = \sum_{y \in Q} d(y)$（因 y 遍历 Q，所以 xy 也遍历 Q）．因 $(m,n) = 1$，存在整数 s 和 t 使得 $sn + tm = 1$．因此，

$$d(x) = snd(x) + tmd(x) = snd(x),$$

这是因为 $d(x) \in K$，从而 $md(x) = 0$．所以，

$$d(x) = s\Delta - xs\Delta.$$

808 令 $a_0 = -s\Delta$，可知 d 是主导子． ■

去掉定理 10.29 中 K 是阿贝尔群的假设比去掉定理 10.21 中的这个假设困难得多．我们先证明如果 K 或 Q 是可解群，则补都是共轭的．因 $|Q|$ 和 $|K|$ 互素，K 和 Q 中至少有一个的阶是奇数．费特-汤普森定理说每个奇数阶群都是可解的，从而完成证明．

除了舒尔-扎森豪斯引理之外，在群论中同调还有其他的应用．例如，如果 G 是群，$a \in G$，$\gamma_a: g \mapsto aga^{-1}$ 是由 a 形成的共轭，则对一切 n 有 $\gamma_a^n: g \mapsto a^n g a^{-n}$. 因此，如果 a 的阶为素数 p 且 $a \notin Z(G)$，则 γ_a 是 p 阶自同构．W. Gaschütz 的一个定理用上同调证明每个有限非阿贝尔 p-群有一个 p 阶自同构，它不是由 G 的一个元素形成的共轭．

我们仔细考虑已经产生的公式．

因子组：$0 = xf(y,z) - f(xy,z) + f(x,yz) - f(x,y)$

上边缘：$f(x,y) = xh(y) - h(xy) + h(x)$

导子：$0 = xd(y) - d(xy) + d(x)$

主导子：$d(x) = xa_0 - a_0$

这些公式都涉及交错和；因子组和导子似乎是核，而上边缘和主导子似乎是象．我们把这一点表达得更精确．

记 Q 的 n 个复制的笛卡儿积为 Q^n；为清楚起见，记 Q^n 中的元素为 $[x_1,\cdots,x_n]$ 以替代 $(x_1,\cdots,x_n)$. 因子组和上边缘是某种函数 $Q^2\to K$，导子是某种函数 $Q^1\to K$. 设 F_n 是以 Q^n 为基的自由左 $\mathbf{Z}Q$-模. 根据基的定义，每个函数 $f:Q^n\to K$ 给出扩张 f 的唯一 Q-同态 $\tilde{f}:F_n\to K$，这是因为 K 是 Q-模；即如果 $\mathbf{Set}(Q^n,K)$ 表示集合范畴中一切函数 $Q^n\to K$ 的族，则 $f\mapsto\tilde{f}$ 给出双射

$$\mathbf{Set}(Q^n,K)\to \mathrm{Hom}_{\mathbf{Z}Q}(F_n,K).$$

这个函数的逆是由 $\mathrm{res}:g\mapsto g\mid Q^n$ 定义的限制

$$\mathrm{res}:\mathrm{Hom}_{\mathbf{Z}Q}(F_n,K)\to\mathbf{Set}(Q^n,K).$$

我们现在定义由各个公式引发的映射：

$$d_3:F_3\to F_2:d_3[x,y,z]=x[y,z]-[xy,z]+[x,yz]-[x,y];$$
$$d_2:F_2\to F_1:d_2[x,y]=x[y]-[xy]+[x].$$

事实上，还要多定义一个映射：设 $Q^0=\{1\}$ 是 1-点集，从而 $F_0=\mathbf{Z}Q$ 是单一生成元 1 上的自由 Q-模. 现在定义

$$d_1:F_1\to F_0:d_1[x]=x-1.$$

我们已经在自由模的基上定义了 d_3,d_2 和 d_1，从而它们的每一个都可扩张成一个 Q-映射. [809]

命题 10.30 *序列*

$$F_3\xrightarrow{d_3}F_2\xrightarrow{d_2}F_1\xrightarrow{d_1}F_0$$

是 Q-模的正合列.

证明概要 我们只验证 $d_1d_2=0$ 和 $d_2d_3=0$；即 $\mathrm{im}\,d_2\subseteq\ker d_1$ 和 $\mathrm{im}\,d_3\subseteq\ker d_2$.（难处理的）反包含将在引入某个同调代数之后，再在定理 10.117 中证明

$$\begin{aligned}d_1d_2[x,y]&=d_1(x[y]-[xy]+[x])\\&=xd_1[y]-d_1[xy]+d_1[x]\\&=x(y-1)-(xy-1)+(x-1)\\&=0\end{aligned}$$

（等式 $d_1x[y]=xd_1[y]$ 成立是因为 d_1 是 Q-映射）. 读者应注意这个计算和命题 10.16 中的一样.

$$\begin{aligned}d_2d_3[x,y,z]&=d_2(x[y,z]-[xy,z]+[x,yz]-[x,y])\\&=xd_2[y,z]-d_2[xy,z]+d_2[x,yz]-d_2[x,y]\\&=x(y[z]-[yz]+[y])-(xy[z]-[xyz]+[xy])\\&\quad+(x[yz]-[xyz]+[x])-(x[y]-[xy]+[x])\\&=0.\end{aligned}$$

■

回忆如果 X 是集合且 K 是模，则函数 $X\to K$ 和同态 $F\to K$ 相同，其中 F 是以 X 为基的自由模：正式地说，函子 $\mathbf{Set}(X,\ )$ 和 $\mathrm{Hom}(F,\ )$，它们映射 ${}_{\mathbf{Z}Q}\mathbf{Mod}\to\mathbf{Set}$，是自然等价的. 运用反变函子 $\mathrm{Hom}_{\mathbf{Z}Q}(\ ,K)$ 到命题 10.30 中的序列上，可得（不必正合）序列

$$\mathrm{Hom}(F_3,K)\xleftarrow{d_3^*}\mathrm{Hom}(F_2,K)\xrightarrow{d_2^*}\mathrm{Hom}(F_1,K)\xleftarrow{d_1^*}\mathrm{Hom}(F_0,K);$$

插入双射 $\mathrm{res}:g\mapsto g\mid Q^n$ 得到集合的交换图：

$$\begin{array}{ccccccc}\mathbf{Set}(Q^3,K)&\leftarrow&\mathbf{Set}(Q^2,K)&\leftarrow&\mathbf{Set}(Q,K)&\leftarrow&\mathbf{Set}(\{1\},K)\\ \uparrow\mathrm{res}&&\uparrow\mathrm{res}&&\uparrow\mathrm{res}&&\uparrow\mathrm{res}\\ \mathrm{Hom}(F_3,K)&\xleftarrow{d_3^*}&\mathrm{Hom}(F_2,K)&\xleftarrow{d_2^*}&\mathrm{Hom}(F_1,K)&\xleftarrow{d_1^*}&\mathrm{Hom}(F_0,K)\end{array}$$

我们把函数 $f:Q^n \to K$ 看作扩张它的 Q-映射 $\tilde{f}:F_n \to K$ 的限制．假设 $f:Q^2 \to K$ 在 $\ker d_3^*$ 中，则 $0 = d_3^*(f) = fd_3$．因此，对一切 $x,y,z \in Q$，有

$$\begin{aligned} 0 &= fd_3[x,y,z] \\ &= f(x[y,z]-[xy,z]+[x,yz]-[x,y]) \\ &= xf[y,z]-f[xy,z]+f[x,yz]-f[x,y]; \end{aligned}$$

810

等式 $f(x[y,z]) = xf[y,z]$ 成立是因为 f 是一个 Q-映射的限制．于是，f 是因子组．如果 f 在 $\operatorname{im} d_2^*$ 中，则存在某个 $h:Q \to K$ 满足 $f = d_2^*(h) = hd_2$．于是，

$$\begin{aligned} f[x,y] &= hd_2[x,y] \\ &= h(x[y]-[xy]+[x]) \\ &= xh[y]-h[xy]+h[x]; \end{aligned}$$

等式 $h(x[y]) = xh[y]$ 成立是因为 h 是一个 Q-映射的限制．从而，f 是一个上边缘．

类似的分析表明，如果 $g:Q \to K$ 在 $\ker d_2^*$ 中，则 g 是导子．现在我们计算 $\operatorname{im} d_1^*$．如果 $k:\{1\} \to K$，则

$$d_1^*(k) = kd_1(x) = k((x-1)1) = (x-1)k(1),$$

这是因为 k 是一个 Q-映射的限制．现在 $k(1)$ 只是 K 的一个元素；确实，如果把 k 等同于它的（1-点）象 $k(1) = a_0$，则我们看到 $d_1^*(k)$ 是主导子．

考虑 $d_2d_3 = 0$ 蕴涵 $d_3^* d_2^* = 0$，后者和 $\operatorname{im} d_2^* \subseteq \ker d_3^*$ 等价；即每个上边缘都是因子组，这正是命题 10.16. 类似地，$d_1d_2 = 0$ 蕴涵 $\operatorname{im} d_1^* \subseteq \ker d_2^*$；即每个主导子都是导子，这是例10.25(ⅰ).

既然我们计算核和象，什么是 $\ker d_1^*$？如果 $k:\{1\} \to K$ 和 $K(1) = a_0$，则 $k \in \ker d_1^*$ 说

$$0 = d_1^*(k) = kd_1(x) = (x-1)k(1) = (x-1)a_0,$$

从而对一切 $x \in Q$ 有 $xa_0 = a_0$．我们已经引出下面的定义．

定义 如果 Q 是群和 K 是 Q-模，则**不动点**子模定义为

$$H^0(Q,K) = \{a \in K : xa = a, \text{对一切 } x \in Q\}.$$

群 $H^2(Q,K)$, $H^1(Q,K)$ 和 $H^0(Q,K)$ 是运用函子 $\operatorname{Hom}(\ ,K)$ 到正合列 $F_3 \to F_2 \to F_1 \to F_0$ 上得到的．在代数拓扑中，也可以用函子 $\otimes_{\mathbb{Z}Q}K$ 得到**同调群**［因为可以像例8.79(ⅴ)那样，把自由 Q-模F_n 看作右 Q-模，所以张量积有定义］：

$$\begin{aligned} H_0(Q,K) &= \ker(d_0 \otimes 1)/\operatorname{im}(d_1 \otimes 1); \\ H_1(Q,K) &= \ker(d_1 \otimes 1)/\operatorname{im}(d_2 \otimes 1); \\ H_2(Q,K) &= \ker(d_2 \otimes 1)/\operatorname{im}(d_3 \otimes 1). \end{aligned}$$

可以证明 $H_0(Q,K)$ 是 K 的极大 Q-平凡商．在把 $K = \mathbb{Z}$ 看作平凡 Q-模的特殊情形中，我们看到 $H_1(Q,\mathbb{Z}) \cong Q/Q'$，其中 Q'是 Q 的换位子群．

811

下一节我们讨论同调代数，要了解以上这些构造，它才是真正的背景．

习题

10.13 设 Q 是群，并设 K 是 Q-模．证明 K 和 Q 的任两个实现算子的分裂扩张等价．

10.14 设 Q 是群，并设 K 是 Q-模．

（ⅰ）如果 K 和 Q 都是有限群，证明 $H^2(Q,K)$ 也是有限的．

（ⅱ）令 $\tau(K,Q)$ 表示出现在 K 和 Q 的实现算子的扩张中的非同构中间群 G 的个数．证明

$$\tau(K,Q) \leqslant |H^2(Q,K)|.$$

（ⅲ）举出一个例子证明（ⅱ）中的不等式可以是严格的．

提示：考虑 $\tau(\mathbb{I}_p,\mathbb{I}_p)=2$（注意，因为每个 p^2 阶群都是阿贝尔群，所以核是平凡模）．

10.15　回忆例 5.79：**广义四元数群 $\mathbf{Q}_n$** 是 2^n 阶群，其中 $n \geqslant 3$，它由两个元素 a 和 b 生成，且满足

$$a^{2^{n-1}}=1, bab^{-1}=a^{-1} \text{ 和 } b^2=a^{2^{n-2}}.$$

（ⅰ）证明 $\mathbf{Q}_n$ 有唯一的 2 阶元素 z，且 $Z(\mathbf{Q}_n)=\langle z\rangle$．由此推出 $\mathbf{Q}_n$ 不是半直积．

（ⅱ）证明 $\mathbf{Q}_n$ 是 $\mathbb{I}_2$ 和 $D_{2^{n-1}}$ 的**中心扩张**（即 θ 是平凡的）．

（ⅲ）用因子组给出 $\mathbf{Q}_n$ 的存在性的另一个证明．

10.16　如果 p 是奇素数，证明每个 $2p$ 阶群 G 都是 $\mathbb{I}_p$ 和 $\mathbb{I}_2$ 的半直积，并由此推出 G 或者是循环群，或者 $G\cong D_{2p}$．

10.17　证明每个 12 阶群 G 同构于下面 5 个群之一：

$$\mathbb{I}_{12}, \mathbf{V}\times\mathbb{I}_3, A_4, S_3\times\mathbb{I}_2, T,$$

其中 T 是例 10.9 中的群．

10.18　如果 Q 是群和 K 是 Q-模，设 E 是 K 和 Q 的半直积，并设 $\ell: G\to E$ 是提升．证明 $\ell(x)=(d(x),x)$，其中 $d:Q\to K$，且 ℓ 是同态当且仅当 d 是导子．

10.19　如果 $U:{}_{\mathbb{Z}Q}\mathbf{Mod}\to\mathbf{Set}$ 是底函子（给每个模指派它的元素的集合），证明有序对 (Φ,U) 是函子的伴随对．［根据习题7.39(ⅱ)，存在**自由函子** $\Phi:\mathbf{Set}\to{}_{\mathbb{Z}Q}\mathbf{Mod}$，它给每个集合 X 指派以 X 为基的自由 Q-模 $\Phi(X)$．］

10.20　证明函子 $\mathbf{Set}(X,\ )$ 和 $\mathrm{Hom}(\Phi,\ )$ 自然等价，它们映射${}_{\mathbb{Z}Q}\mathbf{Mod}\to\mathbf{Set}$，其中 Φ 是习题 10.19 中定义的自由函子．

812

10.4　同调函子

设 R 是环．本节中，模这个字总是指"左 R-模"．给定模 M，存在自由模 F_0 和满射 $\epsilon:F_0\to M$；于是，存在正合列

$$0\to\Omega_1\xrightarrow{i}F_0\xrightarrow{\epsilon}M\to 0,$$

其中 $\Omega_1=\ker\epsilon$ 和 $i:\Omega_1\to F_0$ 是包含映射．这正是用另一种方法来描述 M 的表现，即用生成元和关系来描述 M 的表现．于是，如果 X 是 F_0 的基，则我们说 X[或 $\epsilon(X)$] 是 M 的生成元且 Ω_1 是关系．现在的思想是取生成元和 Ω_1 中的关系，以获得"二阶关系"Ω_2，并迭代这个构造获得 M 的一个自由分解，它可以看作用生成元和关系描述的 M 的更详尽的表现．在代数拓扑中，拓扑空间 X 被链群的序列代替，且这个序列产生同调群 $H_n(X)$．我们现在要用 R-模 M 的一个分解来代替 M.

定义　模 M 的一个**投射分解**是指一个正合列，

$$\cdots\to P_n\to P_{n-1}\to\cdots\to P_1\to P_0\to M\to 0,$$

其中每个模 P_n 都是投射的．一个**自由分解**是指一个投射分解，其中每个模 P_n 都是自由的．

命题 10.30 呈示了自由左 $\mathbb{Z}Q$-模的正合列

$$F_3\xrightarrow{d_3}F_2\xrightarrow{d_2}F_1\xrightarrow{d_1}F_0,$$

其中 F_n 是以 Q^n 为基的自由 Q-模．模 $F_0=\mathbb{Z}Q$ 是生成元 1 上的自由模，且映射 $d_1:F_1\to\mathbb{Z}Q$ 由

$$d_1:[x]\mapsto x-1$$

给出．

命题 10.31　对任意群 Q，存在同构 $\mathbb{Z}Q/\mathrm{im}d_1 \cong \mathbb{Z}$，其中$\mathbb{Z}$看作平凡 Q-模．

证明　定义 $\varepsilon: \mathbb{Z}Q \to \mathbb{Z}$ 为

$$\varepsilon: \sum_{x\in Q} m_x x \mapsto \sum_{x\in Q} m_x.$$

现在 ε 是 Q-映射，这是因为如果 $x \in Q$，则 $\varepsilon(x) = 1$；另一方面，因为$\mathbb{Z}$是平凡 Q-模，所以 $\varepsilon(x) = \varepsilon(x \cdot 1) = x\varepsilon(1) = 1$．显然 ε 是满射且 $\mathrm{im}d_1 \leqslant \ker\varepsilon$［因为 $\varepsilon(x-1) = 0$］．关于反包含，如果 $\sum_{x\in Q} m_x x \in \ker\varepsilon$，则 $\sum_{x\in Q} m_x = 0$．因此，

813

$$\sum_{x\in Q} m_x x = \sum_{x\in Q} m_x x - \Big(\sum_{x\in Q} m_x\Big)1 = \sum_{x\in Q} m_x (x-1) \in \mathrm{im}d_1.$$

所以，$\mathrm{coker}d_1 = \mathbb{Z}Q/\mathrm{im}d_1 \cong \mathbb{Z}$．■

于是，命题 10.30 中的正合列可以加长使得它以 $\mathrm{coker}d_1 = \mathbb{Z}Q/\mathrm{im}d_1$ 结尾，从而看起来像是平凡 Q-模$\mathbb{Z}$的自由分解的起始．

命题 10.32　每个模 M 都有自由分解（且因此有投射分解）．

证明　和 10.1 节中一样，存在自由模 F_0 和正合列

$$0 \to \Omega_1 \xrightarrow{i_1} F_0 \xrightarrow{\varepsilon} M \to 0.$$

类似地，存在自由模 F_1、满射 $\varepsilon_1: F_1 \to \Omega_1$ 和正合列

$$0 \to \Omega_2 \xrightarrow{i_2} F_1 \xrightarrow{\varepsilon_1} \Omega_1 \to 0.$$

定义 $d_1: F_1 \to F_0$ 为复合 $i_1\varepsilon_1$．显然 $\mathrm{im}d_1 = \Omega_1 = \ker\varepsilon$ 且 $\ker d_1 = \Omega_2$，从而存在正合列

$$\begin{array}{ccccccccc} & & F_1 & \xrightarrow{d_1} & F_0 & \xrightarrow{\varepsilon} & M & \to & 0 \\ & \nearrow & & \searrow^{\varepsilon_1} & \nearrow_{i_1} & & & & \\ 0 \to \Omega_2 & & & & \Omega_1 & & & & \end{array}$$

显然这个构造可以对 $n \geqslant 0$ 迭代（从而最终的正合列是无限长的）．■

有一个对偶构造．

定义　模 M 的一个**内射分解**是指一个正合列

$$0 \to M \to E^0 \to E^1 \to \cdots \to E^n \to E^{n+1} \to \cdots,$$

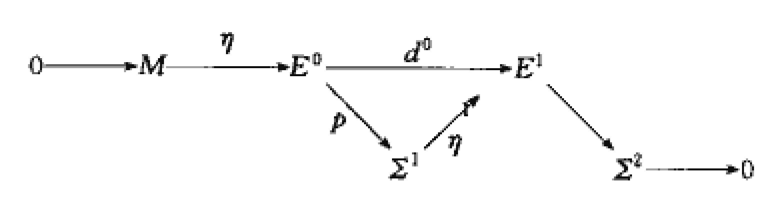
其中每个模 E^n 都是内射模．

命题 10.33　每个模 M 都有内射分解．

证明　我们用定理 8.104，它说明每个模都能够作为子模嵌入一个内射模．于是，存在内射模 E^0、内射 $\eta: M \to E^0$ 和正合列

$$0 \to M \xrightarrow{\eta} E^0 \xrightarrow{p} \Sigma^1 \to 0,$$

其中 $\Sigma^1 = \mathrm{coker}\,\eta$ 和 p 是自然映射．现在重复：存在内射模 E^1，嵌入 $\eta^1: \Sigma^1 \to E^1$，产生正合列



814

其中 d^0 是复合 $d^0 = \eta^1 p$．这个构造可以迭代．■

我们现在推广这两个定义．

定义 一个复形[^1]（$\mathbf{C}_\bullet, d_\bullet$）是指模和映射的一个序列，对每个 $n \in \mathbb{Z}$，

$$\mathbf{C}_\bullet = \cdots \to C_{n+1} \xrightarrow{d_{n+1}} C_n \xrightarrow{d_n} C_{n-1} \to \cdots,$$

其中对一切 $n, d_n d_{n+1} = 0$．映射 d_n 叫做**微分**．

通常，我们把记号（$\mathbf{C}_\bullet, d_\bullet$）缩写为 $\mathbf{C}_\bullet$．

注意等式 $d_n d_{n+1} = 0$ 等价于

$$\mathrm{im} d_{n+1} \subseteq \ker d_n.$$

例 10.34 （i）每个正合列都是一个复形，这是因为要求的包含关系 $\mathrm{im} d_{n+1} \subseteq \ker d_n$ 现在是等式 $\mathrm{im} d_{n+1} = \ker d_n$．

（ii）三角剖分空间 X 的链群的序列

$$\cdots \to C_3(X) \xrightarrow{\partial_3} C_2(X) \xrightarrow{\partial_2} C_1(X) \xrightarrow{\partial_1} C_0(X)$$

是一个复形．然而，复形要假设对每个 $n \in \mathbb{Z}$ 有一个模．我们对一切负的 n 定义 $C_n(X) = \{0\}$ 迫使它成为复形；对 $n \leqslant 0$ 定义微分 $d_n: C_n(X) \to C_{n-1}(X)$ 是没有问题的，因为从任一模到 $\{0\}$ 只有零映射．

（iii）在第 9 章中，我们考虑了 $\mathbb{R}^n$ 的一个连通开子集 X 的德拉姆复形：

$$0 \to \Omega^0(X) \xrightarrow{d^0} \Omega^1(X) \xrightarrow{d^1} \Omega^2(X) \to \cdots \to \Omega^{n-1}(X) \xrightarrow{d^{n-1}} \Omega^n(X) \to 0,$$

其中映射是外导数．

（iv）**零复形 $\mathbf{0}_\bullet$** 是指复形（$\mathbf{C}_\bullet, d_\bullet$），它的每个项 $C_n = \{0\}$，且必然地，它的每个微分 $d_n = 0$．

（v）如果 $\{M_n : n \in \mathbb{Z}\}$ 是模的任意序列，如果对一切 n 定义 $d_n = 0$，则（$\mathbf{M}_\bullet, d_\bullet$）是第 n 项为 M_n 的复形．

（vi）每个同态都是微分．如果 $f: A \to B$ 是同态，定义复形（$\mathbf{C}_\bullet, d_\bullet$）满足 $C_1 = A, C_0 = B, d_1 = f$，其他的项和其他的微分都是零．

（vii）对模 M 的每个投射分解

$$\cdots \to P_1 \to P_0 \to M \to 0,$$

如果在右边加 $\{0\}$，则它是一个复形．

815

（viii）对模 M 的每个内射分解

$$0 \to M \to E^0 \to E^1 \to \cdots,$$

如果在左边加 $\{0\}$，则它是一个复形．

我们使用了一个方便的记号．按照复形的定义，微分降低指标：$d_n: C_n \to C_{n-1}$．满足定义的最简单的方法是用负指标：定义 $C_{-n} = E^n$，从而

$$0 \to M \to C_0 \to C_{-1} \to C_{-2} \to \cdots$$

是一个复形．

（ix）如果 $\mathbf{C}_\bullet$ 是复形，

$$\mathbf{C}_\bullet = \cdots \to C_n \xrightarrow{d_n} C_{n-1} \to \cdots,$$

又如果 F 是加性（共变）函子，比如 $F: {}_R\mathbf{Mod} \to \mathbf{Ab}$，则由

$$F(\mathbf{C}_\bullet) = \cdots \to F(C_n) \xrightarrow{Fd_n} F(C_{n-1}) \to \cdots$$

[^1]: ⊖ 在文献中也叫做链复形．

定义的 $F(\mathbf{C}_\bullet)$ 也是复形：

$$0 = F(0) = F(d_n d_{n+1}) = F(d_n)F(d_{n+1});$$

等式 $0 = F(0)$ 成立是因为 F 是加性函子．注意，即使原来的复形是正合的，函子复形 $F(\mathbf{C}_\bullet)$也可能不是正合的．

（x）如果 F 是反变加性函子，$F(\mathbf{C}_\bullet)$ 是复形的结果仍然为真，但我们必须排列记号使得微分降低指标 1. 更详细地说，应用 F 之后，有

$$F(\mathbf{C}_\bullet) = \cdots \leftarrow F(C_n) \xleftarrow{Fd_n} F(C_{n-1}) \leftarrow \cdots;$$

微分 Fd_n 增加指标 1. 引入负指标几乎解决了这个问题．如果定义 $X_{-n} = F(C_n)$，则序列重写为

$$F(\mathbf{C}_\bullet) = \cdots \to X_{-n+1} \xrightarrow{Fd_n} X_{-n} \to \cdots.$$

然而，映射的指标应该是 $-n+1$，而不是 n. 定义

$$\delta_{-n+1} = Fd_n.$$

重新标号的序列现在读起来是恰当的：

$$F(\mathbf{C}_\bullet) = \cdots \to X_{-n+1} \xrightarrow{\delta_{-n+1}} X_{-n} \to \cdots.$$

然而，负指标是笨拙的，下面是惯用的记号：改变指标的符号并把它提升为上标：记

816

$$\delta^n = \delta_{-n}.$$

函子序列的最终形式现在是这样的：

$$F(\mathbf{C}_\bullet) = \cdots \to X^{n-1} \xrightarrow{\delta^{n-1}} X^n \to \cdots.$$

■

考虑一切复形的范畴可带来方便，因此我们引入它的态射．

定义 如果 $(\mathbf{C}_\bullet, d_\bullet)$ 和 $(\mathbf{C}'_\bullet, d'_\bullet)$ 都是复形，则一个**链映射**

$$f = f_\bullet : (\mathbf{C}_\bullet, d_\bullet) \to (\mathbf{C}'_\bullet, d'_\bullet)$$

是指映射 $f_n : C_n \to C'_n$ 对一切 $n \in \mathbb{Z}$ 的序列，它使得下图交换：

$$\begin{array}{ccccccccc}
\cdots \longrightarrow & C_{n+1} & \xrightarrow{d_{n+1}} & C_n & \xrightarrow{d_n} & C_{n-1} & \longrightarrow \cdots \\
& \downarrow{\scriptstyle f_{n+1}} & & \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n-1}} & \\
\cdots \longrightarrow & C'_{n+1} & \xrightarrow{d'_{n+1}} & C'_n & \xrightarrow{d'_n} & C'_{n-1} & \longrightarrow \cdots
\end{array}$$

容易验证两个链映射

$$f_\bullet : (\mathbf{C}_\bullet, d_\bullet) \to (\mathbf{C}'_\bullet, d'_\bullet) \text{ 和 } \quad g_\bullet : (\mathbf{C}'_\bullet, d'_\bullet) \to (\mathbf{C}''_\bullet, d''_\bullet)$$

的复合 gf 本身也是一个链映射，其中 $(gf)_n = g_n f_n$. $(\mathbf{C}_\bullet, d_\bullet)$ 上的恒等链映射 $1_{\mathbf{C}_\bullet}$ 是恒等映射 $1_{C_n} : C_n \to C_n$ 的序列．

定义 如果 R 是环，则一切左 R-模复形的范畴记为 ${}_R\mathbf{Comp}$；如果环 R 是清楚的，则可以省略 R.

对范畴 **Comp**，如果定义

$$\text{对一切 } n \in \mathbb{Z}, (f+g)_n = f_n + g_n,$$

则 **Comp** 是预加性范畴（即 Hom 都是阿贝尔群且只要可能分配律就成立）.

下面的定义模仿 10.1 节中三角剖分空间的同调群的构造．

定义 如果$(\mathbf{C}_\bullet, d_\bullet)$是复形，定义

$$n\text{-圈} = Z_n(\mathbf{C}_\bullet) = \ker d_n;$$

$$n\text{-边界} = B_n(\mathbf{C}_\bullet) = \mathrm{im}\, d_{n+1}.$$

因在复形中等式 $d_n d_{n+1}=0$ 等价于条件

$$\mathrm{im}\, d_{n+1} \subseteq \ker d_n,$$

所以对每个复形 $\mathbf{C}_\bullet$ 有 $B_n(\mathbf{C}_\bullet) \subseteq Z_n(\mathbf{C}_\bullet)$．

817

定义　如果 $\mathbf{C}_\bullet$ 是复形，$n \in \mathbb{Z}$，它的 n 次**同调**是指

$$H_n(\mathbf{C}_\bullet) = Z_n(\mathbf{C}_\bullet)/B_n(\mathbf{C}_\bullet).$$

例 10.35　一个复形是正合列当且仅当它的一切同调群都是$\{0\}$：即对一切 n，$H_n(\mathbf{C}_\bullet)=\{0\}$．于是，同调群度量复形背离正合列的程度．正合列常叫做**无圈复形**，无圈的意思是没有不是边界的圈．■

例 10.36　在例10.34(ⅵ)中，我们看到每个同态 $f:A\to B$ 可以看作一个复形 $\mathbf{C}_\bullet$ 的一部分，其中 $C_1=A, C_0=B, d_1=f$，左右两边都是$\{0\}$．现在 $d_2=0$ 蕴涵 $\mathrm{im}\, d_2=0$，$d_0=0$ 蕴涵 $\ker d_0=B$；由此

$$H_n(\mathbf{C}_\bullet) = \begin{cases} \ker f & \text{如果 } n=1; \\ \mathrm{coker} f & \text{如果 } n=0; \\ \{0\} & \text{其他.} \end{cases}$$

■

命题 10.37　对每个 $n\in\mathbb{Z}$，同调 $H_n: {}_R\mathbf{Comp}\to {}_R\mathbf{Mod}$ 是加性函子．

证明　我们刚才在对象上定义了 H_n；剩下要在态射上定义 H_n．如果 $f:(\mathbf{C}_\bullet, d_\bullet)\to(\mathbf{C}'_\bullet, d'_\bullet)$ 是链映射，定义 $H_n(f): H_n(\mathbf{C}_\bullet)\to H_n(\mathbf{C}'_\bullet)$ 为

$$H_n(f): z_n + B_n(\mathbf{C}_\bullet) \mapsto f_n z_n + B_n(\mathbf{C}'_\bullet).$$

我们需要证明 $f_n z_n$ 是一个圈且 $H_n(f)$ 不依赖于圈 z_n 的选取；这两者都来自 f 是链映射；即来自下图的交换性：

$$\begin{array}{ccccc} C_{n+1} & \xrightarrow{d_{n+1}} & C_n & \xrightarrow{d_n} & C_{n-1} \\ {\scriptstyle f_{n+1}}\downarrow & & {\scriptstyle f_n}\downarrow & & \downarrow{\scriptstyle f_{n-1}} \\ C'_{n+1} & \xrightarrow[d'_{n+1}]{} & C'_n & \xrightarrow[d'_n]{} & C'_{n-1} \end{array}$$

首先，设 z 是 $Z_n(\mathbf{C}_\bullet)$ 中的 n-圈，从而 $d_n z=0$．图的交换性给出

$$d'_n f_n z = f_{n-1} d_n z = 0.$$

所以，$f_n z$ 是 n-圈．

其次，假定 $z+B_n(\mathbf{C}_\bullet)=y+B_n(\mathbf{C}_\bullet)$；因此，$z-y\in B_n(\mathbf{C}_\bullet)$；即有某个 $c\in C_{n+1}$ 使得

$$z-y=d_{n+1}c.$$

818

应用 f_n 得

$$f_n z - f_n y = f_n d_{n+1} c = d'_{n+1} f_{n+1} c \in B_n(\mathbf{C}'_\bullet).$$

于是，$f_n z + B_n(\mathbf{C}'_\bullet) = f_n y + B_n(\mathbf{C}'_\bullet)$．

我们证明 H_n 是函子．显然 $H_n(1_{\mathbf{C}_\bullet})$ 是恒等映射．如果 f 和 g 是链映射且它们的复合 gf 有定义，则对每个 n-圈 z，有

$$\begin{aligned} H_n(gf): z+B \mapsto & (gf)_n(z+B) \\ &= g_n f_n(z+B) \\ &= H_n(g)(f_n z + B) \\ &= H_n(g)H_n(f)(z+B). \end{aligned}$$

最后，H_n 是加性的：如果 $g:(\mathbf{C}_\bullet,d_\bullet)\to(\mathbf{C}'_\bullet,d'_\bullet)$ 是另一个链映射，则

$$\begin{aligned}H_n(f+g): z+B_n(\mathbf{C}_\bullet) &\mapsto (f_n+g_n)z+B_n(\mathbf{C}'_\bullet)\\ &= f_nz+g_nz+B_n(\mathbf{C}'_\bullet)\\ &= (H_n(f)+H_n(g))(z+B_n(\mathbf{C}'_\bullet)).\end{aligned}$$

■

定义 称 $H_n(f)$ 为**诱导映射**，常把它记为 f_{n*}，或者甚至是 f_*.

命题 10.38 设 R 和 A 是环，并设 $T:{}_R\mathbf{Mod}\to{}_A\mathbf{Mod}$ 是正合加性函子．则 T 和同调可交换；即对每个复形 $(\mathbf{C}_\bullet,d_\bullet)\in{}_R\mathbf{Comp}$ 和每个 $n\in\mathbb{Z}$，存在同构

$$H_n(T\mathbf{C}_\bullet,Td_\bullet)\cong TH_n(\mathbf{C}_\bullet,d_\bullet).$$

证明 考虑底下一行正合的交换图，

$$\begin{array}{ccccccccc} & & C_{n+1} & \xrightarrow{d_{n+1}} & C_n & \xrightarrow{d_n} & C_{n-1} & & \\ & & {\scriptstyle d'_{n+1}}\downarrow & & \uparrow{\scriptstyle k} & & & & \\ 0 & \to & \operatorname{im}d_{n+1} & \xrightarrow{j} & \ker d_n & \to & H_n(\mathbf{C}_\bullet) & \to & 0\end{array}$$

其中 j 和 k 都是包含映射，d'_{n+1} 就是 d_{n+1}，只不过把 d_{n+1} 的目标域从 C_n 改为 $\operatorname{im}d_{n+1}$. 运用正合函子 T 得到底下一行正合的交换图

819

$$\begin{array}{ccccccccc} & & TC_{n+1} & \xrightarrow{Td_{n+1}} & TC_n & \xrightarrow{Td_n} & TC_{n-1} & & \\ & & {\scriptstyle Td'_{n+1}}\downarrow & & \uparrow{\scriptstyle Tk} & & & & \\ 0 & \to & T(\operatorname{im}d_{n+1}) & \xrightarrow{Tj} & T(\ker d_n) & \to & TH_n(\mathbf{C}_\bullet) & \to & 0\end{array}$$

另一方面，因为 T 是正合的，有 $T(\operatorname{im}d_{n+1})=\operatorname{im}T(d_{n+1})$ 和 $T(\ker d_n)=\ker(Td_n)$，从而底下一行是

$$0\to\operatorname{im}(Td_{n+1})\to\ker(Td_n)\to TH_n(\mathbf{C}_\bullet)\to 0.$$

根据定义，$\ker(Td_n)/\operatorname{im}(Td_{n+1})=H_n(T\mathbf{C}_\bullet)$，从而根据命题 8.93，$H_n(T\mathbf{C}_\bullet)\cong TH_n(\mathbf{C}_\bullet)$.

■

现在我们引入拓扑中形成的一个概念．

定义 如果一个链映射 $f:(\mathbf{C}_\bullet,d_\bullet)\to(\mathbf{C}'_\bullet,d'_\bullet)$ 对一切 n 存在映射 $s_n:A_n\to A'_{n+1}$ 使得

$$f_n=d'_{n+1}s_n+s_{n-1}d_n.$$

$$\begin{array}{ccccccccc}\cdots & \to & A_{n+1} & \xrightarrow{d_{n+1}} & A_n & \xrightarrow{d_n} & A_{n-1} & \to & \cdots\\ & & {\scriptstyle f_{n+1}}\downarrow & \swarrow{\scriptstyle s_n} & {\scriptstyle f_n}\downarrow & \swarrow{\scriptstyle s_{n-1}} & \downarrow{\scriptstyle f_{n-1}} & & \\ \cdots & \to & A'_{n+1} & \xrightarrow{d'_{n+1}} & A'_n & \xrightarrow{d'_n} & A'_{n-1} & \to & \cdots\end{array}$$

则称链映射 f 为**零伦的**．如果 $f,g:(\mathbf{C}_\bullet,d_\bullet)\to(\mathbf{C}'_\bullet,d'_\bullet)$ 是链映射，且 $f-g$ 是零伦的，则称 f 和 g **同伦**[⊖]，记为 $f\simeq g$.

命题 10.39 同伦链映射诱导出同调群之间相同的同态：如果 $f,g:(\mathbf{C}_\bullet,d_\bullet)\to(\mathbf{C}'_\bullet,d'_\bullet)$ 都是链映射且 $f\simeq g$，则

⊖ 设 $f,g:X\to Y$ 是两个连续函数，如果 f 能够"变形"到 g 中，即存在连续函数 $F:X\times\mathbf{I}\to Y$，其中 $\mathbf{I}=[0,1]$ 是单位闭区间，使得对一切 $x\in X$ 有 $F(x,0)=f(x)$ 和 $F(x,1)=g(x)$，则称 f 和 g 同伦．现在每个连续函数 $f:X\to Y$ 诱导出同态 $f_*:H_n(X)\to H_n(Y)$，可以证明，如果 f 和 g 同伦，则 $f_*=g_*$．这里给出的同伦的代数定义是从这个拓扑定理的证明中提取出来的．

$$f_{*n} = g_{*n}: H_n(\mathbf{C}_\bullet) \to H_n(\mathbf{C}'_\bullet).$$

证明　如果 z 是 n-圈，则 $d_n z = 0$ 且

$$f_n z - g_n z = d'_{n+1} s_n z + s_{n-1} d_n z = d'_{n+1} s_n z.$$

所以，$f_n z - g_n z \in B_n(\mathbf{C}'_\bullet)$，因此，$f_{*n} = g_{*n}$. ■

定义　如果一个复形（$\mathbf{C}_\bullet, d_\bullet$）的恒等映射 $1_{\mathbf{C}_\bullet}$ 是零伦的，则称该复形有**压缩同伦**⊖. [820]

命题 10.40　有压缩同伦的复形（$\mathbf{C}_\bullet, d_\bullet$）是无圈的；即它是一个正合列.

证明　用例 10.35. 现在 $1_{\mathbf{C}_\bullet}: H_n(\mathbf{C}_\bullet) \to H_n(\mathbf{C}_\bullet)$ 是恒等映射，而 $0_*: H_n(\mathbf{C}_\bullet) \to H_n(\mathbf{C}_\bullet)$ 是零映射. 然而，因 $1_{\mathbf{C}_\bullet} \simeq 0$，这两个映射是相同的. 由此，对一切 $n, H_n(\mathbf{C}_\bullet) = \{0\}$；即对一切 $n, \ker d_n = \operatorname{im} d_{n+1}$，这是正合性的定义. ■

一旦完成平凡 $\mathbb{Z}Q$-模$\mathbb{Z}$ 的自由分解，这个平凡 $\mathbb{Z}Q$-模$\mathbb{Z}$ 的最先几项已由命题 10.30（也可参见命题 10.31）给出，我们便可以通过证明作为阿贝尔群的复形它有压缩同伦，从而证明它是一个正合列.

为了研究同调函子，必须了解它们的定义域 $\mathbf{Comp}_{R}\mathbf{Mod}$ 中的许多构造在 $\mathbf{Comp}$ 范畴中也可以做. 我们只列出定义和陈述某种性质，验证是简单的练习，留给读者.

（ⅰ）$\mathbf{Comp}$ 中的一个**同构**是这个范畴中的一个等价. 读者应验证链映射 $f: \mathbf{C}_\bullet \to \mathbf{C}'_\bullet$ 是同构当且仅当对一切 $n \in \mathbb{Z}, f_n: C_n \to C'_n$ 是$_R\mathbf{Mod}$ 中的同构.（我们必须验证逆 f_n^{-1} 的序列是一个链映射；即相应的图交换.）

（ⅱ）设($\mathbf{C}_\bullet, d_\bullet$)是一个复形，如果对每个 $n \in \mathbb{Z}$，A_n 是 C_n 的子模且 $\delta_n = d_n | A_n$，则称($\mathbf{A}_\bullet, \delta_\bullet$)是（$\mathbf{C}_\bullet, d_\bullet$）的一个**子复形**.

如果 $i_n: A_n \to C_n$ 是包含映射，则易知 $\mathbf{A}_\bullet$ 是 $\mathbf{C}_\bullet$ 的子复形当且仅当 $i: \mathbf{A}_\bullet \to \mathbf{C}_\bullet$ 是链映射.

（ⅲ）如果 $\mathbf{A}_\bullet$ 是 $\mathbf{C}_\bullet$ 的子复形，则**商复形**是指

$$\mathbf{C}_\bullet/\mathbf{A}_\bullet = \cdots \to C_n/A_n \xrightarrow{d''_n} C_{n-1}/A_{n-1} \to \cdots,$$

其中 $d''_n: c_n + A_n \mapsto d_n c_n + A_{n-1}$（必须证明 d''_n 是合理定义的：如果 $c_n + A_n = b_n + A_n$，则 $d_n c_n + A_{n-1} = d_n b_n + A_{n-1}$）. 如果 $\pi_n: C_n \to C_n/A_n$ 是自然映射，则 $\pi: \mathbf{C}_\bullet \to \mathbf{C}_\bullet/\mathbf{A}_\bullet$ 是链映射.

（ⅳ）如果 $f_\bullet: (\mathbf{C}_\bullet, d_\bullet) \to (\mathbf{C}'_\bullet, d'_\bullet)$是链映射，定义

$$\mathbf{ker} f = \cdots \to \ker f_{n+1} \xrightarrow{\delta_{n+1}} \ker f_n \xrightarrow{\delta_n} \ker f_{n-1} \to \cdots,$$

其中 $\delta_n = d_n | \ker f_n$，并定义

$$\mathbf{im} f = \cdots \to \operatorname{im} f_{n+1} \xrightarrow{\Delta_{n+1}} \operatorname{im} f_n \xrightarrow{\Delta_n} \operatorname{im} f_{n-1} \to \cdots,$$

其中 $\Delta_n = d'_n | \operatorname{im} f_n$. 易知 $\mathbf{ker} f$ 是 $\mathbf{C}_\bullet$ 的子复形，$\mathbf{im} f$ 是 $\mathbf{C}'_\bullet$ 的子复形，且**第一同构定理**成立：

$$\mathbf{C}_\bullet/\mathbf{ker}\, f \cong \mathbf{im} f.$$

[821]

（ⅴ）称复形和链映射的一个序列

$$\cdots \to \mathbf{C}^{n+1}_\bullet \xrightarrow{f^{n+1}} \mathbf{C}^n_\bullet \xrightarrow{f^n} \mathbf{C}^{n-1}_\bullet \to \cdots$$

是**正合列**，如果对一切 $n \in \mathbb{Z}$，

$$\mathbf{im} f^{n+1} = \mathbf{ker} f^n.$$

我们可以验证，如果 $\mathbf{A}_\bullet$ 是 $\mathbf{C}_\bullet$ 的子复形，则存在复形的正合列

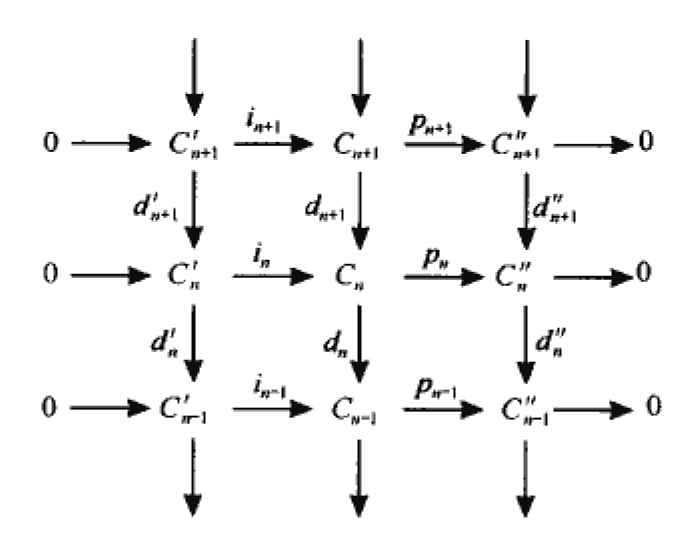
⊖ 如果一个拓扑空间的恒等映射同伦于一个常数映射，则称该拓扑空间为可缩的.

$$\mathbf{0}_\bullet \to \mathbf{A}_\bullet \xrightarrow{i} \mathbf{C}_\bullet,$$

其中 $\mathbf{0}_\bullet$ 是零复形，i 是包含链映射．更一般地，如果 $i:\mathbf{C}_\bullet \to \mathbf{C}'_\bullet$ 是链映射，则每个 i_n 是单射当且仅当存在正合列 $\mathbf{0}_\bullet \to \mathbf{C}_\bullet \xrightarrow{i} \mathbf{C}'_\bullet$．类似地，如果 $p:\mathbf{C}_\bullet \to \mathbf{C}''_\bullet$ 是链映射，则每个 p_n 是满射当且仅当存在正合列

$$\mathbf{C}_\bullet \xrightarrow{p} \mathbf{C}''_\bullet \to \mathbf{0}_\bullet.$$

读者应明白这个记号是非常简洁的．例如，如果把一个复形写成列，则一个复形的短正合列事实上是有正合行的无限交换图：



复形的序列 $\cdots \to \mathbf{C}_\bullet^{n+1} \xrightarrow{f^{n+1}} \mathbf{C}_\bullet^{n} \xrightarrow{f^{n}} \mathbf{C}_\bullet^{n-1} \to \cdots$ 是正合的当且仅当对每个 $m \in \mathbb{Z}$，

$$\cdots \to C_m^{n+1} \to C_m^{n} \to C_m^{n-1} \to \cdots$$

822 是一个模的正合列．

（vi）如果 $\{(\mathbf{C}_\bullet^{\alpha}, d_\bullet^{\alpha})\}$ 是复形的族，则它们的直和是复形

$$\sum_\alpha \mathbf{C}_\bullet^{\alpha} = \cdots \to \sum_\alpha C_{n+1}^{\alpha} \xrightarrow{\sum_\alpha d_n^\alpha} \sum_\alpha C_n^{\alpha} \xrightarrow{\sum_\alpha d_{n-1}^\alpha} \sum_\alpha C_{n-1}^{\alpha} \to \cdots,$$

其中 $\sum_\alpha d_n^\alpha$ 的作用是坐标状态的；即 $\sum_\alpha d_n^\alpha:(c_n^\alpha)\mapsto(d_n^\alpha c_n^\alpha)$.

总之，可以把 **Comp** 看作和模范畴本质上有相同性质的范畴；其实，应该把复形看作一个广义模．（诸如 $_R$**Mod** 和 **Comp** 这样的范畴叫做**阿贝尔范畴**．）

下面的初等构造是基本的；它给出不同的同调模之间的一个关系．其证明是一系列图上追踪法．通常，我们要说证明是平淡的，但因为结果的重要性，我们把证明详细（或许太详细）地呈示出来；作为简单证明的示意，我们略去下标．

命题 10.41（连接同态） 如果

$$\mathbf{0}_\bullet \to \mathbf{C}'_\bullet \xrightarrow{i} \mathbf{C}_\bullet \xrightarrow{p} \mathbf{C}''_\bullet \to \mathbf{0}_\bullet$$

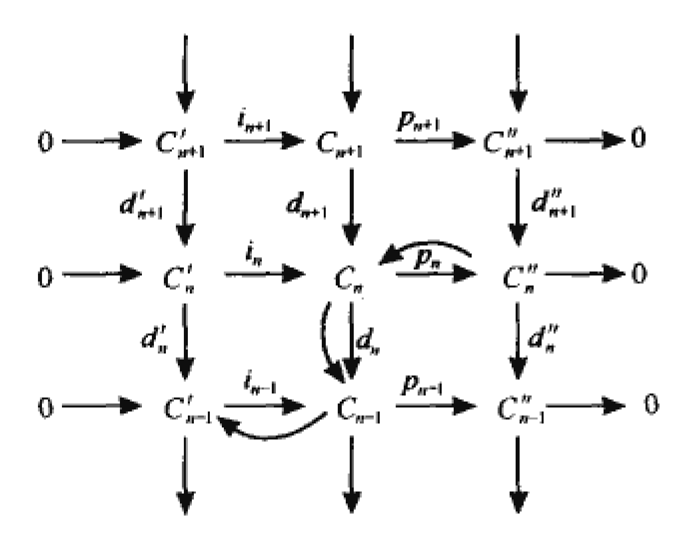
是复形的正合列，则对每个 $n\in\mathbb{Z}$，存在由

$$\partial_n: z''_n + B_n(\mathbf{C}''_\bullet) \mapsto i_{n-1}^{-1} d_n p_n^{-1} z''_n + B_{n-1}(\mathbf{C}'_\bullet)$$

定义的同态

$$\partial_n: H_n(\mathbf{C}''_\bullet) \to H_{n-1}(\mathbf{C}'_\bullet).$$

证明 在这个证明中，我们要缩写许多记号．考虑有正合行的交换图：



假设 $z'' \in C''_n$ 和 $d''z'' = 0$．因 p_n 是满射，存在 $c \in C_n$ 使得 $pc = z''$．现在把 c 下推到 $dc \in C_{n-1}$．根据交换性，$p_{n-1}dc = d''p_nc = d''z'' = 0$，从而 $dc \in \ker p_{n-1} = \mathrm{im}\, i_{n-1}$ 因为 i_{n-1} 是单射，所以存在唯一的 $c' \in C'_{n-1}$ 使得 $i_{n-1}c' = dc$. 于是，$i_{n-1}^{-1}dp_n^{-1}z''$有意义；即断言 [823]

$$\partial_n(z'' + B''_n) = c' + B'_{n-1}$$

是合理定义的同态．

首先，我们证明不依赖于提升的选取．假设 $p_n\check{c} = z''$，其中$\check{c} \in C_n$. 则 $c - \check{c} \in \ker p_n = \mathrm{im}\, i_n$，因此存在 $u' \in C'_n$使得 $i_nu' = c - \check{c}$. 根据第一个方块的交换性，有

$$i_{n-1}d'u' = di_nu' = dc - d\check{c}.$$

因此，$i^{-1}dc - i^{-1}d\check{c} = d'u' \in B'_{n-1}$；即 $i^{-1}dc + B'_{n-1} = i^{-1}d\check{c} + B'_{n-1}$. 于是，这个公式给出合理定义的函数

$$Z''_n \to C'_{n-1}/B'_{n-1}.$$

其次，函数 $Z''_n \to C'_{n-1}/B'_{n-1}$是同态．如果 z''，$z''_1 \in Z''_n$，令 $pc = z''$和 $pc_1 = z''_1$. 因 ∂ 的定义不依赖于提升的选取，选取 $c + c_1$ 为 $z'' + z''_1$的一个提升．现在这个步骤可以简单地完成．

再次，我们证明如果 $i_{n-1}c' = dc$ 则 c'是一个圈：$0 = ddc = dic' = idc'$，且因 i 是单射，从而 $d'c' = 0$. 因此公式给出同态

$$Z'' \to Z'/B' = H_{n-1}.$$

最后，子群 B''_n进入 B'_{n-1}. 假定 $z'' = d''c''$，其中 $c'' \in C''_{n+1}$，并设 $pu = c''$，其中 $u \in C_{n+1}$. 交换性给出 $pdu = d''pu = d''c'' = z''$. 因 $\partial(z'')$ 不依赖于提升的选取，我们选取 du 使得 $pdu = z''$，从而 $\partial(z'' + B'') = i^{-1}d(du) + B' = B'$. 所以，公式确实给出同态 $\partial_n: H_n(\mathbf{C}''_\bullet) \to H_{n-1}(\mathbf{C}'_\bullet)$. ■

我们要问的第一个问题是同调函子对复形的一个短正合列的作用是什么．下一个定理也由图上追踪法证明，由于结果很重要我们也给出过于详细的证明．读者应该在阅读我们给出的证明之前，先试着自己证明这个定理．

定理 10.42 (长正合列)　如果

$$\mathbf{0}_\bullet \to \mathbf{C}'_\bullet \xrightarrow{i} \mathbf{C}_\bullet \xrightarrow{p} \mathbf{C}''_\bullet \to \mathbf{0}_\bullet$$

是复形的正合列，则存在模的正合列

$$\cdots \to H_{n+1}(\mathbf{C}''_\bullet) \xrightarrow{\partial_{n+1}} H_n(\mathbf{C}'_\bullet) \xrightarrow{i_*} H_n(\mathbf{C}_\bullet) \xrightarrow{p_*} H_n(\mathbf{C}''_\bullet) \xrightarrow{\partial_n} H_{n-1}(\mathbf{C}'_\bullet) \to \cdots.$$ [824]

证明　这个证明也是平淡的．我们的记号是缩写的，有 6 个包含关系要验证．

（i）$\mathrm{im}\, i_* \subseteq \ker p_*$.

$$p_* i_* = (pi)_* = 0_* = 0$$

(ⅱ) $\ker p_* \subseteq \mathrm{im}\, i_*$.

如果 $p_*(z+B) = pz+B''=B''$，则有某个 $c''\in C''_{n+1}$ 使得 $pz=d''c''$. 但 p 是满射给出某个 $c\in C_{n+1}$ 使得 $c''=pc$，因此 $pz=d''pc=pdc$，这是因为 p 是链映射，从而 $p(z-dc)=0$. 根据正合性，存在 $c'\in C'_n$ 使得 $ic'=z-dc$. 现在因为 z 是一个圈，$id'c'=dic'=dz-ddc=0$，所以 c' 是圈；因 i 是单射，$d'c'=0$. 所以，

$$i_*(c'+B') = ic'+B = z-dc+B = z+B.$$

(ⅲ) $\mathrm{im}\, p_* \subseteq \ker \partial$.

如果 $p_*(c+B)=pc+B''\in \mathrm{im}\, p_*$，则 $\partial(pz+B'')=z'+B'$，其中 $iz'=dp^{-1}pz$. 因这个公式不依赖于 pz 的提升的选取，我们选取 $p^{-1}pz = z$. 现在因为 z 是圈，所以有 $dp^{-1}pz=dz=0$. 于是，$iz'=0$，因为 i 是单射，因此 $z'=0$.

(ⅳ) $\ker \partial \subseteq \mathrm{im}\, p_*$.

如果 $\partial(z''+B'')=B'$，则 $z'=i^{-1}dp^{-1}z''\in B'$；即有某个 $c'\in C'$ 使得 $z'=d'c'$. 但 $iz'=id'c'=dic'=dp^{-1}z''$，因此 $d(p^{-1}z''-ic')=0$；即 $p^{-1}z''-ic'$ 是圈．此外，因原始序列的正合性，有 $pi=0$，从而

$$p_*(p^{-1}z''-ic'+B) = pp^{-1}z''-pic'+B'' = z''+B''.$$

(ⅴ) $\mathrm{im}\, \partial \subseteq \ker i_*$.

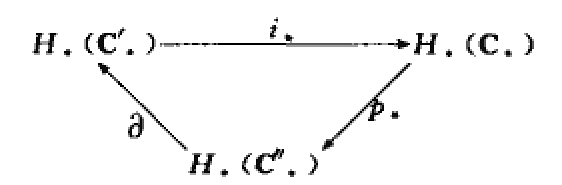
我们有 $i_*\partial(z''+B'') = iz'+B'$，其中 $iz' = dp^{-1}z'' \in B$；即 $i_*\partial = 0$.

(ⅵ) $\ker i_* \subseteq \mathrm{im}\, \partial$.

如果 $i_*(z'+B')=iz'+B=B$，则有某个 $c\in C$ 使得 $iz'=dc$. 因 p 是链映射，根据原始序列的正合性，$d''pc=pdc=piz'=0$，从而 pc 是圈．但

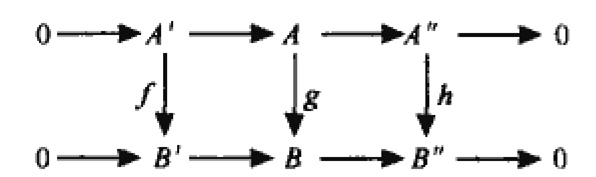
$$\partial(pc+B'') = i^{-1}dp^{-1}pc+B' = i^{-1}dc+B' = i^{-1}iz'+B' = z'+B'.$$ ■

定理 10.42 由于图



825 而常称为正合三角形．

系 10.43 (蛇引理) 给定模的有正合行的交换图，



存在正合列

$$0 \to \ker f \to \ker g \to \ker h \to \mathrm{coker} f \to \mathrm{coker} g \to \mathrm{coker} h \to 0.$$

证明 如果把每个垂直映射 f，g 和 h 看作复形 [如同在例10.34(ⅵ)中一样]，则给定的交换图可以看作复形的短正合列．这些复形中的每一个的同调群只有两个非零项：例如，例 10.36 表明第一列的同调群是 $H_1=\ker f$，$H_0=\mathrm{coker} f$，其他一切 $H_n=\{0\}$．现在从长正合列立即可得蛇引理． ■

定理 10.44 (∂的自然性) 给定复形的有正合行的交换图：

$$\begin{array}{ccccccccc}
\mathbf{0}_\bullet & \longrightarrow & \mathbf{C}'_\bullet & \xrightarrow{i} & \mathbf{C}_\bullet & \xrightarrow{p} & \mathbf{C}''_\bullet & \longrightarrow & \mathbf{0}_\bullet \\
 & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\
\mathbf{0}_\bullet & \longrightarrow & \mathbf{A}'_\bullet & \xrightarrow{j} & \mathbf{A}_\bullet & \xrightarrow{q} & \mathbf{A}''_\bullet & \longrightarrow & \mathbf{0}_\bullet
\end{array}$$

存在模的有正合行的交换图：

$$\begin{array}{ccccccccccc}
\cdots & \longrightarrow & H_n(\mathbf{C}'_\bullet) & \xrightarrow{i_*} & H_n(\mathbf{C}_\bullet) & \xrightarrow{p_*} & H_n(\mathbf{C}''_\bullet) & \xrightarrow{\partial} & H_{n-1}(\mathbf{C}'_\bullet) & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle f_*} & & \downarrow{\scriptstyle g_*} & & \downarrow{\scriptstyle h_*} & & \downarrow{\scriptstyle f_*} & & \\
\cdots & \longrightarrow & H_n(\mathbf{A}'_\bullet) & \xrightarrow{j_*} & H_n(\mathbf{A}_\bullet) & \xrightarrow{q_*} & H_n(\mathbf{A}''_\bullet) & \xrightarrow{\partial'} & H_{n-1}(\mathbf{A}'_\bullet) & \longrightarrow & \cdots
\end{array}$$

证明　行的正合性是定理 10.42，而前两个方块的交换性来自 H_n 是函子．为证明涉及连接同态的方块的交换性，我们先把链映射和微分在一个（3-维）图中表示出来：

$$\begin{array}{ccccccccc}
0 & \longrightarrow & C'_n & \xrightarrow{i} & C_n & \xrightarrow{p} & C''_n & \longrightarrow & 0 \\
 & & {\scriptstyle d'}\swarrow\ \downarrow{\scriptstyle f_\bullet} & & {\scriptstyle d}\swarrow\ \downarrow{\scriptstyle g_\bullet} & & {\scriptstyle d''}\swarrow\ \downarrow{\scriptstyle h_\bullet} & & \\
0 & \longrightarrow & C'_{n-1} & \xrightarrow{i} & C_{n-1} & \xrightarrow{p} & C''_{n-1} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f_\bullet} & & \downarrow{\scriptstyle g_\bullet} & & \downarrow{\scriptstyle h_\bullet} & & \\
0 & \longrightarrow & A'_n & \xrightarrow{j} & A_n & \xrightarrow{q} & A''_n & \longrightarrow & 0 \\
 & & {\scriptstyle \delta'}\swarrow & & {\scriptstyle \delta}\swarrow & & {\scriptstyle \delta''}\swarrow & & \\
0 & \longrightarrow & A'_{n-1} & \xrightarrow{j} & A_{n-1} & \xrightarrow{q} & A''_{n-1} & \longrightarrow & 0
\end{array}$$

如果 $z''+B(\mathbf{C}''_\bullet)\in H_n(\mathbf{C}''_\bullet)$，必须证明　　826

$$f_*\partial(z''+B(\mathbf{C}''_\bullet)) = \partial' h_*(z''+B(\mathbf{C}''_\bullet)).$$

设 $c\in C_n$ 是 z'' 的提升；即 $pc=z''$．现在 $\partial(z''+B(\mathbf{C}''_\bullet))=z'+B(\mathbf{C}'_\bullet)$，其中 $iz'=dc$. 因此，$f_*\partial(z''+B(\mathbf{A}''_\bullet))=fz'+B(\mathbf{A}'_\bullet)$．另一方面，因 h 是链映射，有 $qgc=hpc=hz''$．在 $\partial'(hz''+B(\mathbf{A}''_\bullet))$ 的计算中，选取 gc 为 hz'' 的提升．因此，$\partial'(hz''+B(\mathbf{A}''_\bullet))=u'+B(\mathbf{A}'_\bullet)$，其中 $ju'=\delta gc$．但

$$jfz'=giz'=gdc=\delta gc=ju',$$

因为 j 是单射，所以 $fz'=u'$．■

在下一节中我们将运用这些一般结果．

习题

10.21　如果 $\mathbf{C}_\bullet$ 是复形，且有某个 n 使得 $C_n=\{0\}$，证明 $H_n(\mathbf{C}_\bullet)=\{0\}$．

10.22　证明同构的复形有相同的同调：如果 $\mathbf{C}_\bullet$ 和 $\mathbf{D}_\bullet$ 同构，则对一切 n, $H_n(\mathbf{C}_\bullet)\cong H_n(\mathbf{D}_\bullet)$．

10.23　如同例10.34(vi)中一样，把定义为 $d: m\mapsto 2m$ 的映射 $d:\mathbb{Z}\to\mathbb{Z}$ 看作一个复形．证明在${}_{\mathbb{Z}}\mathbf{Comp}$ 范畴中它不是一个投射对象，即使它的每个项都是投射$\mathbb{Z}$-模．

10.24　把$\mathbb{Z}$看作对象是整数的 $\mathbf{PO}(\mathbb{Z})$ 范畴，且只要 $n\leqslant m$，就恰有一个态射 $n\to m$，除此没有其他态射．[如果把$\mathbb{Z}$看作一个偏序集，则它是例7.25(v)中定义的相伴范畴．] 证明一个复形 $(\mathbf{C}_\bullet, d_\bullet)$ 是一个反变函子 $\mathbf{PO}(\mathbb{Z})\to{}_R\mathbf{Mod}$，且链映射是自然变换．

10.25　在本题中，我们证明蛇引理蕴涵长正合列（逆命题是系 10.43)．考虑行正合的交换图（注意这个图中"失去"两个零)：

$$\begin{array}{ccccccc}
 & & A & \longrightarrow & B & \xrightarrow{p} & C & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\
0 & \longrightarrow & A' & \xrightarrow{i} & B' & \longrightarrow & C' & &
\end{array}$$

(i) 证明由

$$\Delta : z \mapsto i^{-1}\beta p^{-1} z + \mathrm{im}\alpha$$

定义的 $\Delta: \ker\gamma \to \mathrm{coker}\alpha$ 是合理定义的同态．

（ⅱ）证明存在正合列

827

$$\ker\alpha \to \ker\beta \to \ker\gamma \xrightarrow{\Delta} \mathrm{coker}\alpha \to \mathrm{coker}\beta \to \mathrm{coker}\gamma.$$

（ⅲ）给定有正合行的交换图，

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A_n' & \longrightarrow & A_n & \longrightarrow & A_n'' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d_n'} & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d_n''} & & \\
0 & \longrightarrow & A_{n-1}' & \longrightarrow & A_{n-1} & \longrightarrow & A_{n-1}'' & \longrightarrow & 0
\end{array}$$

证明下面的图交换且有正合行：

$$\begin{array}{ccccccccc}
 & & A_n'/\mathrm{im}d_{n+1}' & \longrightarrow & A_n/\mathrm{im}d_{n+1} & \longrightarrow & A_n''/\mathrm{im}d_{n+1}'' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d'} & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d''} & & \\
0 & \longrightarrow & \ker d_{n-1}' & \longrightarrow & \ker d_{n-1} & \longrightarrow & \ker d_{n-1}'' & &
\end{array}$$

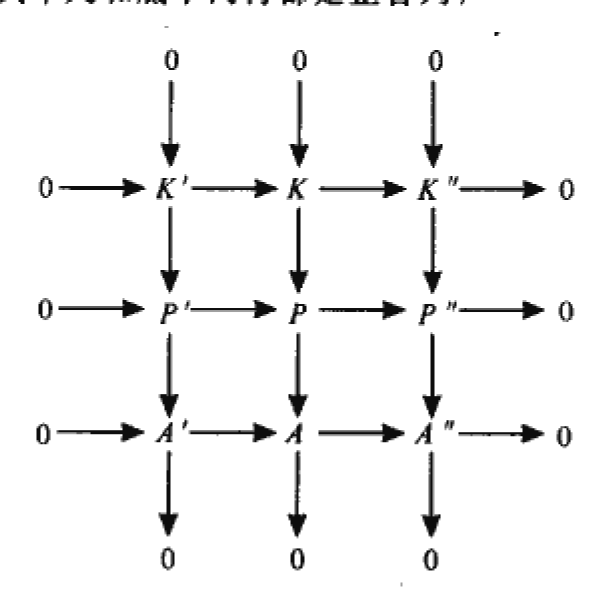
（ⅳ）用（ⅱ）和上面的图给出长正合列的另一个证明．

10.26　设 $f,g: \mathbf{C}_\bullet \to \mathbf{C}_\bullet'$ 是链映射，并设 $F: \mathbf{C}_\bullet \to \mathbf{C}_\bullet'$ 是加性函子．如果 $f \simeq g$，证明 $Ff \simeq Fg$；即如果 f 和 g 同伦，则 Ff 和 Fg 同伦．

10.27　设 $\mathbf{0}_\bullet \to \mathbf{C}_\bullet' \xrightarrow{i} \mathbf{C}_\bullet \xrightarrow{p} \mathbf{C}_\bullet'' \to \mathbf{0}_\bullet$ 是复形的正合列，其中 $\mathbf{C}_\bullet'$ 和 $\mathbf{C}_\bullet''$ 是无圈的．证明 $\mathbf{C}_\bullet$ 也是无圈的．

10.28　设 $(\mathbf{C}_\bullet, d_\bullet)$ 是复形，它的每个微分 d_n 都是零映射．证明对一切 n, $H_n(\mathbf{C}_\bullet) \cong C_n$．

10.29　（3×3 引理）给定交换图，其中列和底下两行都是正合列，



证明顶上一行也是正合列．

10.30　证明同调与直和可交换：对一切 n，存在自然同构

$$H_n\left(\sum_\alpha \mathbf{C}_\bullet^\alpha\right) \cong \sum_\alpha H_n(\mathbf{C}_\bullet^\alpha).$$

828

10.31　（ⅰ）定义复形 $\{\mathbf{C}_\bullet^i, \varphi_j^i\}$ 的正系统，并证明在 $_R\mathbf{Comp}$ 中 $\varinjlim \mathbf{C}_\bullet^i$ 存在．

（ⅱ）如果 $\{\mathbf{C}_\bullet^i, \varphi_j^i\}$ 是在一个有向指标集上的复形的正系统，证明对一切 $n \geqslant 0$，

$$H_n(\varinjlim \mathbf{C}_\bullet^i) \cong \varinjlim H_n(\mathbf{C}_\bullet^i).$$

10.32　假设 R-模的复形 $(\mathbf{C}_\bullet, d_\bullet)$ 有压缩同伦，其中满足

$$1_{C_n} = d_{n+1}s_n + s_{n-1}d_n$$

的映射 $s_n: C_n \to C_{n+1}$ 是唯一的 $\mathbb{Z}$-映射．证明 $(\mathbf{C}_\bullet, d_\bullet)$ 是正合列．

10.33 （ⅰ）设 $0 \to F_n \to F_{n-1} \to \cdots \to F_0 \to 0$ 是有限生成自由 k-模的正合列，其中 k 是交换环．证明

$$\sum_{i=0}^{n}(-1)^i \operatorname{rank}(F_i)=0.$$

（ⅱ）设

$$0 \to F_n \to F_{n-1} \to \cdots \to F_0 \to M \to 0$$

和

$$0 \to F'_m \to F'_{m-1} \to \cdots \to F'_0 \to M \to 0$$

都是一个 k-模的自由分解，其中一切 F_i 和 F'_j 都是有限生成自由 k-模．证明

$$\sum_{i=0}^{n}(-1)^i \operatorname{rank}(F_i)=\sum_{j=0}^{m}(-1)^j \operatorname{rank}(F'_j).$$

这个公共的值记为 $\chi(M)$，叫做 M 的**欧拉-庞加莱特征**．

提示：用 Schanuel 引理．

假定 k 是 PID.

10.34 （ⅰ）设 $\mathbf{C}_\bullet: 0 \to C_n \to C_{n-1} \to \cdots \to C_0 \to 0$ 是交换环 k 上有限生成自由 k-模的复形．证明

$$\sum_{i=0}^{n}(-1)^i \operatorname{rank}(C_i)=\sum_{i=0}^{n}(-1)^i \operatorname{rank}(H_i(\mathbf{C}_\bullet)).$$

（ⅱ）设 $0 \to M' \to M \to M'' \to 0$ 是 k-模的正合列．如果其中两个模有欧拉-庞加莱特征，证明第三个模也有欧拉-庞加莱特征，且

$$\chi(M)=\chi(M')+\chi(M'').$$

10.35 （ⅰ）（Barratt-Whitehead）．考虑有正合行的交换图：

$$\begin{array}{ccccccccccc}
A_n & \xrightarrow{i_n} & B_n & \xrightarrow{p_n} & C_n & \xrightarrow{\partial_n} & A_{n-1} & \longrightarrow & B_{n-1} & \longrightarrow & C_{n-1} \\
\downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle g_n} & & \downarrow{\scriptstyle h_n} & & \downarrow{\scriptstyle f_{n-1}} & & \downarrow{\scriptstyle g_{n-1}} & & \downarrow{\scriptstyle h_{n-1}} \\
A'_n & \xrightarrow[j_n]{} & B'_n & \xrightarrow[q_n]{} & C'_n & \longrightarrow & A'_{n-1} & \longrightarrow & B'_{n-1} & \longrightarrow & C'_{n-1}
\end{array}$$

829

如果每个 h_n 是一个同构，证明存在正合列

$$A_n \xrightarrow{(f_n,i_n)} A'_n \oplus B_n \xrightarrow{j_n-g_n} B'_n \xrightarrow{\partial_n h_n^{-1} q_n} A_{n-1} \to A'_{n-1} \oplus B_{n-1} \to B'_{n-1},$$

其中 $(f_n,i_n): a_n \mapsto (f_n a_n, i_n a_n)$ 和 $j_n-g_n: (a'_n,b_n) \mapsto j_n a'_n - g_n b_n$.

（ⅱ）（迈尔-菲托里斯）．假定在定理 10.44 的图中，每个第三个垂直映射 h_n 是一个同构．证明存在正合列

$$\cdots \to H_n(\mathbf{C}'_\bullet) \to H_n(\mathbf{A}'_\bullet) \oplus H_n(\mathbf{C}_\bullet) \to H_n(\mathbf{A}_\bullet) \to H_{n-1}(\mathbf{C}'_\bullet) \to \cdots.$$

注：艾伦伯格-斯廷罗德公理刻画了一切拓扑空间和连续映射的 **Top** 范畴上的同调函子．如果 h_n：**Top** $\to$ **Ab** 是函子序列，对一切 $n \geqslant 0$，满足下列条件：长正合列；连接同态的自然性；只要 f 和 g 同伦就有 $h_n(f)=h_n(g)$；当 X 是 1-点空间时，$h_0(X)=\mathbf{Z}$ 和对一切 $n>0, h_n(X)=\{0\}$；以及切除．则对一切 n 存在自然同构 $h_n \to H_n$．切除涉及称为相对同调的一个附加构造，但在其他公理中出现时，切除可以用迈尔-菲托里斯序列的正合性代替．

10.5 导函子

为了运用关于同调的一般结果，我们需要复形的短正合列的一个来源以及它们所处的交换图．思路是用一个模的（删除）分解替代这个模．然后运用 Hom 或⊗以及由此产生的叫做 Ext 或 Tor 的同调模．给定模的一个短正合列，我们将看到可以用分解替代它的每个模，并得到一个复形的短正合列．

本节是相当枯燥的，但为了建立同调函子的存在性却是必需的．本节最有用的定理是定理

10.46（比较定理）、命题 10.50（它证明基本构造是合理定义的）、系 10.57（长正合列）和命题 10.58（连接同态的自然性）.

对于想要立即运用 Tor（张量的左导函子）和 Ext（Hom 的右导函子）的读者以及想要推迟考察箭头迷宫的读者，下一定理给出了刻画函子 Ext^n 的公理集.

定理 10.45 设 $\mathrm{EXT}^n: {}_R\mathbf{Mod} \to \mathbf{Ab}$ 是反变函子的序列，对 $n \geq 0$，满足

（i）对每个短正合列 $0 \to A \to B \to C \to 0$，存在长正合列和自然连接同态

$$\cdots \to \mathrm{EXT}^n(C) \to \mathrm{EXT}^n(B) \to \mathrm{EXT}^n(A) \xrightarrow{\Delta_n} \mathrm{EXT}^{n+1}(C) \to \cdots;$$

830

（ii）存在左 R-模 M 使得 EXT^0 和 $\mathrm{Hom}_R(\ ,M)$ 自然等价；

（iii）对一切投射模 P 和一切 $n \geq 1$，$\mathrm{EXT}^n(P) = \{0\}$.

如果 $\mathrm{Ext}^n(\ ,M)$ 是另一个满足相同公理的反变函子的序列，则对一切 $n \geq 0$，$\mathrm{EXT}^n(\ ,M)$ 自然等价于 Ext^n.

注 在习题 10.44 和习题 10.45 中有共变 Ext 函子和 Tor 函子的公理化描述.

证明 对 $n \geq 0$ 用归纳法证明．基础步是公理（ii）.

关于归纳步，给定模 A，选取短正合列

$$0 \to L \to P \to A \to 0,$$

其中 P 是投射的．根据公理（i），存在行正合的图：

$$\begin{array}{ccccccc}
\mathrm{EXT}^0(P) & \longrightarrow & \mathrm{EXT}^0(L) & \xrightarrow{\Delta_0} & \mathrm{EXT}^1(A) & \longrightarrow & \mathrm{EXT}^1(P) \\
\downarrow{\scriptstyle \tau_P} & & \downarrow{\scriptstyle \tau_L} & & \vdots\downarrow & & \\
\mathrm{Hom}(P,M) & \longrightarrow & \mathrm{Hom}(L,M) & \xrightarrow{\partial_0} & \mathrm{Ext}^1(A,M) & \longrightarrow & \mathrm{Ext}^1(P,M)
\end{array}$$

其中映射 τ_P 和 τ_L 是公理（ii）给出的同构．由于等价 $\mathrm{EXT}^0 \to \mathrm{Hom}(\ ,M)$ 的自然性，这个图交换．根据公理（iii），$\mathrm{Ext}^1(P,M) = \{0\}$ 且 $\mathrm{EXT}^1(P) = \{0\}$．由此映射 Δ_0 和 ∂_0 是满射．这正好是命题 8.93 中的那种图，因此存在同构 $\mathrm{EXT}^1(A) \to \mathrm{Ext}^1(A,M)$ 使得增广的图交换.

现在可以假定 $n \geq 1$，我们进一步关注长正合列．根据公理（i），存在行正合的图

$$\begin{array}{ccccccc}
\mathrm{EXT}^n(P) & \longrightarrow & \mathrm{EXT}^n(L) & \xrightarrow{\Delta_n} & \mathrm{EXT}^{n+1}(A) & \longrightarrow & \mathrm{EXT}^{n+1}(P) \\
 & & \downarrow{\scriptstyle \sigma} & & \vdots\downarrow & & \\
\mathrm{Ext}^n(P,M) & \longrightarrow & \mathrm{Ext}^n(L,M) & \xrightarrow{\partial_n} & \mathrm{Ext}^{n+1}(A,M) & \longrightarrow & \mathrm{Ext}^{n+1}(P,M)
\end{array}$$

其中 $\sigma: \mathrm{EXT}^n(L) \to \mathrm{Ext}^n(L,M)$ 是由归纳假设给出的同构．因 $n \geq 1$，涉及投射模 P 的四个项都是 $\{0\}$；因此由行的正合性，Δ_n 和 ∂_n 都是同构．最后，复合 $\partial_n\sigma\Delta_n^{-1}: \mathrm{EXT}^{n+1}(A) \to \mathrm{Ext}^{n+1}(A,M)$ 是同构.

剩下要证明同构 $\mathrm{EXT}^n(A) \to \mathrm{Ext}^n(A,M)$ 组成自然变换．这里用到公理（i）中连接同态的自然性的假定，其证明留给读者. ■

这种起步缓慢的归纳证明在证明归纳步之前先对 $n=0$ 和 $n=1$ 证明结果，是经常使用的，叫做**长度推移法**.

831

本节的剩余部分是构造满足公理（i）、（ii）和（iii）的函子．我们用导函子证明 Ext 和 Tor 的存在性（也有其他的证明）．由于这些函子是用性质的简短列表刻画的，因此在使用 Ext 和 Tor 时往往可以不必经常了解它们构造的详情.

我们先从一个技术性的定义开始.

定义 如果 $\cdots \to P_2 \to P_1 \xrightarrow{d_1} P_0 \to A \to 0$ 是模 A 的投射分解，则它的**删除投射分解**是复形

$$\mathbf{P}_A = \cdots \to P_2 \to P_1 \to P_0 \to 0.$$

类似地，如果 $0 \to A \to E^0 \xrightarrow{d^0} E^1 \to E^2 \to \cdots$ 是模 A 的内射分解，则**删除内射分解**是复形

$$\mathbf{E}^A = 0 \to E^0 \to E^1 \to E^2 \to \cdots.$$

在两种情形中，删除 A 并没有丢失信息：在第一种情形中 $A \cong \operatorname{coker} d_1$，在第二种情形中 $A \cong \ker d^0$. 当然，一个删除分解不再是正合的：

$$H_0(\mathbf{P}_A) = \ker(P_0 \to \{0\})/\operatorname{im}d_1 = P_0/\operatorname{im}d_1 \cong A.$$

我们知道一个模有许多表现，因此下面的结果是基本的.

定理 10.46（比较定理）　给定映射 $f: A \to A'$，考虑图

$$\begin{array}{ccccccccccc}
\cdots \to & P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} & P_0 & \xrightarrow{\varepsilon} & A & \to 0 \\
 & \downarrow \check{f}_2 & & \downarrow \check{f}_1 & & \downarrow \check{f}_0 & & \downarrow f & \\
\cdots \to & P'_2 & \xrightarrow{d'_2} & P'_1 & \xrightarrow{d'_1} & P'_0 & \xrightarrow{\varepsilon'} & A' & \to 0
\end{array}$$

其中行是复形. 如果顶上一行中的每个 P_n 都是投射的，且如果底下一行是正合的，则存在链映射 $\check{f}: \mathbf{P}_\bullet \to \mathbf{P}'_\bullet$ 使得完成的图交换. 此外，任两个这样的链映射同伦.

注　比较定理的对偶也成立. 此时复形向右侧延伸，顶上一行假定是正合的，底下一行假定除了 A' 之外是内射的.

证明　（i）对 $n \geqslant 0$ 用归纳法证明 $\check{f}_n$ 的存在性. 关于基础步 $n = 0$，考虑图

$$\begin{array}{ccc}
 & & P_0 \\
 & \swarrow & \downarrow f\varepsilon \\
P'_0 & \xrightarrow{\varepsilon'} & A' \to 0
\end{array}$$

832

因 ε' 是满射且 P_0 是投射，存在映射 $\check{f}_0: P_0 \to P'_0$ 使得 $\varepsilon' \check{f}_0 = f\varepsilon$.

关于归纳步，考虑图

$$\begin{array}{ccccc}
P_{n+1} & \xrightarrow{d_{n+1}} & P_n & \xrightarrow{d_n} & P_{n-1} \\
 & & \downarrow \check{f}_n & & \downarrow \check{f}_{n-1} \\
P'_{n+1} & \xrightarrow{d'_{n+1}} & P'_n & \xrightarrow{d'_n} & P'_{n-1}
\end{array}$$

如果能够证明 $\operatorname{im} \check{f}_n d_{n+1} \subseteq \operatorname{im} d'_{n+1}$，则有图

$$\begin{array}{ccc}
 & & P_{n+1} \\
 & \swarrow & \downarrow \check{f}_n d_{n+1} \\
P'_{n+1} & \xrightarrow{d'_{n+1}} & \operatorname{im}d'_{n+1} \to 0
\end{array}$$

P_{n+1} 的投射性将提供映射 $\check{f}_{n+1}: P_{n+1} \to P'_{n+1}$ 使得 $d'_{n+1}\check{f}_{n+1} = \check{f}_n d_{n+1}$. 为验证包含关系成立，注意原始图的底下一行在 P'_n 处的正合性给出 $\operatorname{im}d'_{n+1} = \ker d'_n$，因此只要证明 $d'_n \check{f}_n d_{n+1} = 0$. 但 $d'_n \check{f}_n d_{n+1} = \check{f}_{n-1} d_n d_{n+1} = 0$.

（ii）现在证明如不计同伦 $\check{f}$ 唯一. 如果 $h: \mathbf{P}_\bullet \to \mathbf{P}'_\bullet$ 是链映射也满足 $\varepsilon' h_0 = f\varepsilon$，则对 $n \geqslant 0$ 用归纳法构造同伦 s 的项 $s_n: P_n \to P'_{n+1}$；即我们想要

$$h_n - \check{f}_n = d'_{n+1}s_n + s_{n-1}d_n.$$

现在开始作归纳法．首先定义 $\check{f}_{-1} = f = h_{-1}$. 如果定义 $s_{-1} = 0 = s_{-2}$，则

$$h_{-1} - \check{f}_{-1} = f - f = 0 = d'_0 s_{-1} + s_{-2}d_{-1}$$

对任何 d'_0 和 d_{-1} 成立；定义 $d'_0 = \varepsilon', d_{-1} = 0$.

关于归纳步，只需证明

$$\operatorname{im}(h_{n+1} - \check{f}_{n+1} - s_n d_{n+1}) \subseteq \operatorname{im} d'_{n+2},$$

这是因为我们有行正合的图

$$\begin{array}{ccccc} & & P_{n+1} & & \\ & \swarrow & \downarrow h_{n+1}-\check{f}_{n+1}-s_nd_{n+1} & & \\ P'_{n+2} & \xrightarrow{d'_{n+2}} & \operatorname{im} d'_{n+2} & \longrightarrow & 0 \end{array}$$

833

P_{n+1} 的投射性给出满足所要求等式的映射 $s_{n+1}: P_{n+1} \to P'_{n+2}$. 和（i）的证明一样，原始图底下一行的正合性给出 $\operatorname{im} d'_{n+2} = \ker d'_{n+1}$，从而只需证明

$$d'_{n+1}(h_{n+1} - \check{f}_{n+1} - s_n d_{n+1}) = 0.$$

但

$$\begin{aligned} d'_{n+1}(h_{n+1} - \check{f}_{n+1} - s_n d_{n+1}) &= d'_{n+1}(h_{n+1} - \check{f}_{n+1}) - d'_{n+1}s_n d_{n+1} \\ &= d'_{n+1}(h_{n+1} - \check{f}_{n+1}) - (h_n - \check{f}_n - s_{n-1}d_n)d_{n+1} \\ &= d'_{n+1}(h_{n+1} - \check{f}_{n+1}) - (h_n - \check{f}_n)d_{n+1}, \end{aligned}$$

因为 h 和 $\check{f}$ 都是链映射，所以最后一项是 0. ■

我们引入一个术语描述刚才构造的链映射 $\check{f}$.

定义 如果 $f: A \to A'$ 是模的映射，且如果 $\mathbf{P}_A$ 和 $\mathbf{P}'_{A'}$ 分别是 A 和 A' 的删除投射分解，则链映射 $\check{f}: \mathbf{P}_A \to \mathbf{P}'_{A'}$

$$\begin{array}{ccccccccccc} \cdots \to & P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} & P_0 & \xrightarrow{\varepsilon} & A & \to & 0 \\ & \downarrow \check{f}_2 & & \downarrow \check{f}_1 & & \downarrow \check{f}_0 & & \downarrow f & & \\ \cdots \to & P'_2 & \xrightarrow{d'_2} & P'_1 & \xrightarrow{d'_1} & P'_0 & \xrightarrow{\varepsilon'} & A' & \to & 0 \end{array}$$

称作 f 上的，如果

$$f\varepsilon = \varepsilon' \check{f}_0.$$

于是，比较定理蕴涵：给定同态 $f: A \to A'$，在 A 和 A' 的删除投射分解之间恒存在 f 上的链映射；此外，这样的链映射如不计同伦是唯一的．

给定一对环 R 和 S 以及一个加性共变函子 $T: {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$，我们现在对一切 $n \in \mathbb{Z}$ 构造它的左导函子 $L_nT: {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$.

定义分两部分：首先定义在对象上；然后定义在态射上．

一次选取每个模 A 的一个删除投射分解 $\mathbf{P}_A$．和例 10.34（ix）一样，组成复形 $T\mathbf{P}_A$，并取同调：

$$L_nT(A) = H_n(T\mathbf{P}_A).$$

这个定义由两个例子提出．第一，在代数拓扑中，作三角剖分空间 X 的复形的张量得到系数在

一个阿贝尔群G中的X的同调群$H_n(X,G)$；或者运用Hom(,G)得到一个复形，它的同调群叫做系数在G中的X的上同调群.（当然，后面一个函子是反变的）. 第二，在考虑群扩张时，构成扩张的公式提出构造平凡模Z的自由分解，然后对这个分解运用Hom(,K)或 $\otimes K$.

834

现在定义$L_nT(f)$，其中$f:A\to A'$是同态. 根据比较定理，存在f上的链映射$\check{f}:\mathbf{P}_A\to\mathbf{P}'_A$. 由此，$T\check{f}:T\mathbf{P}_A\to T\mathbf{P}'_{A'}$也是链映射，我们定义$L_nT(f):L_nT(A)\to L_nT(A')$为

$$L_nT(f)=H_n(T\check{f})=(T\check{f})_*.$$

更详细地说，如果$z\in\ker Td_n$，则

$$(L_nT)f:z+\operatorname{im}Td_{n+1}\mapsto(T\check{f}_n)z+\operatorname{im}Td'_{n+1}.$$

用图来说，考虑选定的投射分解：

$$\begin{array}{ccccccccc}\cdots & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & A & \longrightarrow & 0\\ &&&&&& \downarrow f &&\\ \cdots & \longrightarrow & P'_1 & \longrightarrow & P'_0 & \longrightarrow & A' & \longrightarrow & 0\end{array}$$

填上f上的链映射$\check{f}$，删去A和A',对这个图运用T，然后取$T\check{f}$在同调中诱导的映射.

例 10.47　如果$r\in Z(R)$是环R中的一个中心元素，A是左R-模，则定义为$\mu_r:a\mapsto ra$的$\mu_r:A\to A$是一个R-映射. 我们称μ_r为乘r. ■

定义　对共变或反变函子$T:{}_R\mathbf{Mod}\to{}_R\mathbf{Mod}$，如果对一切$r\in Z(R)$,$T(\mu_r):TA\to TA$是乘$r$的映射，则称$T$**保持乘法**.

张量积和Hom保持乘法. 我们断言，如果T保持乘法，则L_nT也保持乘法；即

$$L_nT(\mu_r)=\text{乘 } r.$$

给定投射分解$\cdots\to P_1\xrightarrow{d_1}P_0\xrightarrow{\varepsilon}A\to 0$，易知$\check{\mu}$是$\mu_r$上的链映射，

$$\begin{array}{ccccccccccc}\cdots & \longrightarrow & P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} & P_0 & \xrightarrow{\varepsilon} & A & \longrightarrow & 0\\ && \downarrow\check{\mu}_2 && \downarrow\check{\mu}_1 && \downarrow\check{\mu}_0 && \downarrow f &&\\ \cdots & \longrightarrow & P_2 & \xrightarrow[d_2]{} & P_1 & \xrightarrow[d_1]{} & P_0 & \xrightarrow[\varepsilon]{} & A & \longrightarrow & 0\end{array}$$

其中对每个$n\geqslant 0$,$\check{\mu}_n:P_n\to P_n$是乘r. 因T保持乘法，链映射$T\check{\mu}$的各项都是乘r，因此在同调中的诱导映射也是乘r：

$$(T\check{\mu})_*:z_n+\operatorname{im}Td_{n+1}\mapsto(T\check{\mu}_n)z_n+\operatorname{im}Td_{n+1}=rz_n+\operatorname{im}Td_{n+1},$$

其中$z_n\in\ker Td_n$.

835

命题 10.48　给定一对环R和S以及一个加性共变函子$T:{}_R\mathbf{Mod}\to{}_S\mathbf{Mod}$，则对每个$n$,

$$L_nT:{}_R\mathbf{Mod}\to{}_S\mathbf{Mod}$$

是加性共变函子.

证明　我们证明L_nT在态射上是合理定义的；容易验证它是加性共变函子（记住，H_n是从复形到模的加性共变函子）.

如果$h:\mathbf{P}_A\to\mathbf{P}'_{A'}$是$f$上的另一个链映射，则比较定理说$h\simeq\check{f}$，因此根据习题10.26，$Th\simeq T\check{f}$，从而根据命题10.39，$H_n(Th)=H_n(T\check{f})$. ■

命题 10.49 如果 $T: {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ 是加性共变函子，则对一切负 n 和一切 A，$L_nTA=\{0\}$.

证明 因为当 n 为负时，$\mathbf{P}_A$的第 n 项是 $\{0\}$，所以根据习题 10.21 有 $L_nTA=\{0\}$. ■

定义 如果 B 是左 R-模和 $T = \ \otimes_R B$，定义

$$\mathrm{Tor}_n^R(\ ,B) = L_nT.$$

于是，如果

$$\mathbf{P}_A = \cdots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \to 0$$

是模 A 的选定的删除投射分解，则

$$\mathrm{Tor}_n^R(A,B) = H_n(\mathbf{P}_A \otimes_R B) = \frac{\ker(d_n \otimes 1_B)}{\mathrm{im}(d_{n+1} \otimes 1_B)}.$$

$\mathrm{Tor}_n^R(\ ,B)$ 的定义域是 $\mathbf{Mod}_R$，它是右 R-模的范畴；它的目标域是 $\mathbf{Ab}$，是阿贝尔群的范畴．例如，如果 R 是交换的，则 $A \otimes_R B$ 是 R-模，从而 $\mathrm{Tor}_n^R(\ ,B)$ 的值在 ${}_R\mathbf{Mod}$ 中．

定义 如果 A 是右 R-模和 $T = A \otimes_R$，定义 $\mathrm{tor}_n^R(A,\ ) = L_nT$．于是，如果

$$\mathbf{Q}_B = \cdots \to Q_2 \xrightarrow{d_2} Q_1 \xrightarrow{d_1} Q_0 \to 0$$

是模 B 的选定的删除投射分解，则

$$\mathrm{tor}_n^R(A,B) = H_n(A \otimes_R \mathbf{Q}_B) = \frac{\ker(1_A \otimes d_n)}{\mathrm{im}(1_A \otimes d_{n+1})}.$$

$\mathrm{tor}_n^R(A,\ )$的定义域是 ${}_R\mathbf{Mod}$，它是左 R-模的范畴；它的目标域是 $\mathbf{Ab}$，是阿贝尔群的范畴．和以前一样，它的目标域可以更小（例如，$R=\mathbb{Q}$）或更大［如果 $R=\mathbb{Z}G$，因为每个$\mathbb{Z}$-模可以看作一个（平凡）R-模］．

836

同调代数漂亮的定理之一是对一切 A 和 B（和对一切 R 和 n），有

$$\mathrm{Tor}_n^R(A,B) \cong \mathrm{tor}_n^R(A,B).$$

有运用谱序列的一个证明，但还有一个属于 A. Zaks 的一个初等证明（见 Rotman 所著的《An Introduction to Homological Algebra》，197 页）．

现在有几点要讨论．L_nT 的定义中假定已经选取了每个模的删除投射分解．L_nT 依赖于这个选取吗？并且，一旦解决了这个问题（答案是 L_nT 不依赖于这个选取），如何运用这些函子？

假定选取了新的删除投射分解 $\widetilde{\mathbf{P}}_A$，我们把由这些新的选取形成的左导函子记为 $\widetilde{L}_nT$．

命题 10.50 给定一对环 R 和 S 以及一个加性共变函子 $T: {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$，则对每个 n，函子 L_nT 和 $\widetilde{L}_nT$ 自然等价．特别地，对一切 A，

$$(L_nT)A \cong (\widetilde{L}_nT)A,$$

从而这些模不依赖于 A 的（删除）投射分解的选取．

证明 考虑图

$$\begin{array}{ccccccccc} \cdots \to & P_2 & \to & P_1 & \to & P_0 & \to & A & \to 0 \\ & & & & & & & \downarrow{\scriptstyle 1_A} & \\ \cdots \to & \widetilde{P}_2 & \to & \widetilde{P}_1 & \to & \widetilde{P}_0 & \to & A & \to 0 \end{array}$$

其中顶上一行是用来定义 L_nT 的选定的投射分解，底下一行是用来定义 $\widetilde{L}_nT$ 的．根据比较定理，存在 1_A 上的链映射$\iota: \mathbf{P}_A \to \widetilde{\mathbf{P}}_A$. 运用 T 得 $T1_A = 1_{TA}$ 上的链映射 $T_\iota: T\mathbf{P}_A \to T\widetilde{\mathbf{P}}_A$. 后面一个的链映射对每个 n 诱导出一个同态，

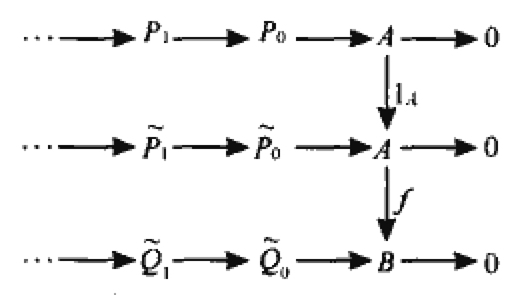
$$\tau_A = (T\iota)_* : (L_nT)A \to (\widetilde{L}_nT)A.$$

我们现在构造 τ_A 的逆以证明每个 τ_A 是同构（从而证明定理中最后一个陈述）. 把前述的图上下倒转，从而选定的投射分解 $\mathbf{P}_A \to A \to 0$ 现在是底下一行. 比较定理再次给出链映射，比如 $\kappa : \widetilde{\mathbf{P}}_A \to \mathbf{P}_A$. 现在复合 $\kappa\iota$ 是 $1_{\mathbf{P}_A}$ 上从 $\mathbf{P}_A$ 到它自身的链映射. 根据比较定理中的唯一性陈述，$\kappa\iota \simeq 1_{\mathbf{P}_A}$；类似地，$\iota\kappa \simeq 1_{\widetilde{\mathbf{P}}_A}$. 由此 $T(\iota\kappa) \simeq 1_{T\widetilde{\mathbf{P}}_A}$ 和 $T(\kappa\iota) \simeq 1_{T\mathbf{P}_A}$. 因此，$1 = (T\iota\kappa)_* = (T\iota)_*(T\kappa)_*$ 和 $1 = (T\kappa\iota)_* = (T\kappa)_*(T\iota)_*$. 所以，$\tau_A = (T\iota)_*$ 是同构. [837]

我们现在证明同构 τ_A 构成自然等价：即如果 $f : A \to B$ 是同态，则下图交换.

$$\begin{array}{ccc} (L_nT)A & \xrightarrow{\tau_A} & (\widetilde{L}_nT)A \\ {\scriptstyle L_nT(f)}\downarrow & & \downarrow{\scriptstyle \widetilde{L}_nT(f)} \\ (L_nT)B & \xrightarrow{\tau_B} & (\widetilde{L}_nT)B \end{array}$$

为了在顺时针方向赋值，考虑



其中底下一行是 B 的某个投射分解. 比较定理给出 $f1_A = f$ 上的链映射 $\mathbf{P}_A \to \widetilde{\mathbf{Q}}_B$. 反时针方向走，$B$ 的选定的投射分解现在是图中的中间行，于是得到 $1_Bf = f$ 上的链映射 $\mathbf{P}_A \to \widetilde{\mathbf{Q}}_B$. 比较定理中的唯一性陈述告诉我们这两个链映射同伦，从而它们给出同调中相同的同态. 于是，相应的图交换，这表明 $\tau : L_nT \to \widetilde{L}_nT$ 是自然等价. ■

系 10.51　*模 $\mathrm{Tor}_n^R(A,B)$ 不依赖于 A 和 B 的投射分解的选取.*

证明　立即运用命题到 $\otimes_R B$ 的左导函子（即 $\mathrm{Tor}_n^R(\ ,B)$）和 $A \otimes_R$ 的左导函子（即 $\mathrm{tor}_n^R(A,\ )$）. 但我们已经引述了 $\mathrm{Tor}_n^R(A,B) \cong \mathrm{tor}_n^R(A,B)$ 的事实. ■

系 10.52　*设 $T : {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ 是加性共变函子. 如果 P 是一个投射模，则对一切 $n \geqslant 1$，$L_nT(P) = \{0\}$.*

特别地，如果 A 和 P 都是右 R-模，且 P 是投射的，又如果 B 和 Q 都是左 R-模，且 Q 是投射的，则对一切 $n \geqslant 1$，

$$\mathrm{Tor}_n^R(P,B) = \{0\} \text{ 和 } \mathrm{Tor}_n^R(A,Q) = \{0\}.$$ [838]

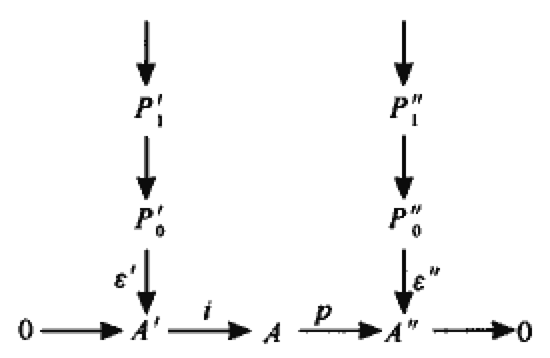
证明　因 P 是投射模，它的投射分解是

$$\mathbf{C}_\bullet = \cdots \to 0 \to 0 \to P \xrightarrow{1_P} P \to 0,$$

因此对应的删除投射分解 $\mathbf{C}_P$ 只有一个非零项，就是 $C_0 = P$. 由此，$T\mathbf{C}_P$ 是对一切 $n \geqslant 1$，第 n 项为 $\{0\}$ 的复形，因此根据习题 10.21，对一切 $n \geqslant 1$，$L_nTP = H_n(T\mathbf{C}_P) = \{0\}$. ■

我们将证明存在左导函子的长正合列. 先从一个有用的引理开始，它说如果给定一个模的正合列以及它的第一项和第三项的投射分解，则可以"钉入蹄铁"；即存在中间项的投射分解正好适合该项.

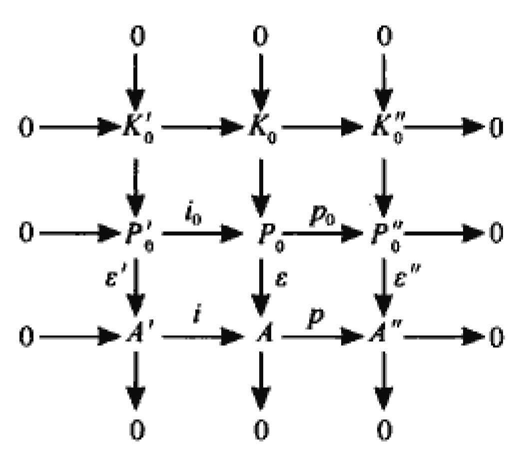
引理 10.53（蹄铁引理）　*给定图*



其中列是投射分解而行是正合的，则存在 A 的投射分解和链映射使得三个列形成复形的正合列．

注 把投射分解换成内射分解的对偶定理也成立．

证明 我们先证明存在投射的 P_0 和有正合的列与行的交换 3×3 图：



839

定义 $P_0 = P'_0 \oplus P''_0$；因为 P'_0 和 P''_0 都是投射的，所以 P_0 也是投射的．定义 $i_0: P'_0 \to P'_0 \oplus P''_0$ 为 $x' \mapsto (x', 0)$，并定义 $p_0: P'_0 \oplus P''_0 \to P''_0$ 为 $(x', x'') \mapsto x''$．显然

$$0 \to P'_0 \xrightarrow{i_0} P_0 \xrightarrow{p_0} P''_0 \to 0$$

是正合的．因 P''_0 是投射的，存在映射 $\sigma: P''_0 \to A$ 使得 $p\sigma = \varepsilon''$．现在定义 $\varepsilon: P_0 \to A$ 为 $\varepsilon: (x', x'') \mapsto i\varepsilon' x' + \sigma x''$．可以证明如果 $K_0 = \ker \varepsilon$，则存在映射 $K'_0 \to K_0$ 和 $K_0 \to K''_0$（其中 $K'_0 = \ker \varepsilon'$ 和 $K''_0 = \ker \varepsilon''$），这留作一个平淡的习题，由此得到的 3×3 图交换．顶上一行的正合性是习题 10.29，而根据五引理，即习题 8.52，ε 是满射．

我们现在对 $n \geqslant 0$ 用归纳法证明可以构造出所要的图的底下 n 行．关于归纳步，假定前 n 步已经填进去了，并设 $K_n = \ker(P_n \to P_{n-1})$，等等．现在构造 3×3 图，它的底下一行是 $0 \to K'_n \to K_n \to K''_n \to 0$，并如下面说明的那样把它和第 n 个图接合起来（注意映射 $P_{n+1} \to P_n$ 定义为复合 $P_{n+1} \to K_n \to P_n$）．

$$\begin{array}{l}
0 \to K'_{n+1} \to K_{n+1} \to K''_{n+1} \to 0 \\
0 \to P'_{n+1} \to P_{n+1} \to P''_{n+1} \to 0 \\
0 \to K'_n \to K_n \to K''_n \to 0 \\
0 \to P'_n \to P_n \to P''_n \to 0 \\
0 \to P'_{n-1} \to P_{n-1} \to P''_{n-1} \to 0
\end{array}$$

新图的列是正合的，这是因为，举例来说，$\operatorname{im}(P_{n+1} \to P_n) = K_n = \ker(P_n \to P_{n-1})$． ■

定理 10.54 如果 $0 \to A' \xrightarrow{i} A \xrightarrow{p} A'' \to 0$ 是模的正合列，又如果 $T: {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ 是共变加性函子，则存在长正合列：

$$\cdots \to L_nTA' \xrightarrow{L_nTi} L_nTA \xrightarrow{L_nTp} L_nTA'' \xrightarrow{\partial_n}$$
$$L_{n-1}TA' \xrightarrow{L_{n-1}Ti} L_{n-1}TA \xrightarrow{L_{n-1}Tp} L_{n-1}TA'' \xrightarrow{\partial_{n-1}} \cdots$$

它以

$$\cdots \to L_0TA' \to L_0TA \to L_0TA'' \to 0$$

结尾.

证明　设 $\mathbf{P}'_{A'}$ 和 $\mathbf{P}''_{A''}$ 分别是 A' 和 A'' 的选定的删除投射分解. 根据引理 10.53，存在 A 的删除投射分解 $\widetilde{\mathbf{P}}_A$ 使得

$$\mathbf{0}. \to \mathbf{P}'_{A'} \xrightarrow{j} \widetilde{\mathbf{P}}_A \xrightarrow{q} \mathbf{P}''_{A''} \to \mathbf{0}.$$

840

（在比较定理的记号中，$j = \check{i}$ 是 i 上的链映射，$q = \check{p}$ 是 p 上的链映射）. 运用 T 得复形的序列

$$\mathbf{0}. \to T\mathbf{P}'_{A'} \xrightarrow{Tj} T\widetilde{\mathbf{P}}_A \xrightarrow{Tq} T\mathbf{P}''_{A''} \to \mathbf{0}..$$

为证明这个序列是正合的，[⊖] 注意每个行 $0 \to P'_n \xrightarrow{j_n} \widetilde{P}_n \xrightarrow{q_n} P''_n \to 0$ 是分裂正合列（因为 P''_n 是投射的），且加性函子保持分裂短正合列. 于是存在长正合列

$$\cdots \to H_n(T\mathbf{P}'_{A'}) \xrightarrow{(Tj)_*} H_n(T\widetilde{\mathbf{P}}_A) \xrightarrow{(Tq)_*} H_n(T\mathbf{P}''_{A''}) \xrightarrow{\partial_n} H_{n-1}(T\mathbf{P}'_{A'}) \to \cdots;$$

即存在正合列

$$\cdots \to L_nTA' \xrightarrow{(Tj)_*} \widetilde{L}_nTA \xrightarrow{(Tq)_*} L_nTA'' \xrightarrow{\partial_n} L_{n-1}TA' \to \cdots.$$

我们不知道由蹄铁引理给出的 A 的投射分解是否是原始选定的分解，这就是为什么我们用 $\widetilde{L}_nTA$ 代替 L_nTA. 但有自然等价 $\tau: L_nT \to \widetilde{L}_nT$，从而存在正合列

$$\cdots \to L_nTA' \xrightarrow{\tau_A^{-1}(Tj)_*} L_nTA \xrightarrow{(Tq)_*\tau_A} L_nTA'' \xrightarrow{\partial_n} L_{n-1}TA' \to \cdots.$$

根据命题 10.49，对一切负 n，$L_{-1}T = \{0\}$，因此上面的序列以 $\{0\}$ 结尾.

剩下要证明 $\tau_A^{-1}(Tj)_* = L_nT(i) = T(j)_*$（记住 $j = \check{i}$，它是 i 上的链映射）和 $(Tq)_*\tau_A = L_nT(p)$. 现在 $\tau_A^{-1} = (T\kappa)_*$，其中 $\kappa: \widetilde{\mathbf{P}}_A \to \mathbf{P}_A$ 是 1_A 上的链映射，因此

$$\tau_A^{-1}(Tj)_* = (T\kappa)_*(Tj)_* = (T\kappa Tj)_* = (T(\kappa j))_*.$$

κj 和 j 都是 1_A 上的链映射 $\widetilde{\mathbf{P}}_A \to \mathbf{P}_A$，从而根据比较定理，它们同伦. 所以，$T(\kappa j)$ 和 Tj 同伦，由此它们在同调中诱导出相同的映射：$(T(\kappa j))_* = (Tj)_* = L_nT(i)$，从而 $\tau_A^{-1}(Tj)_* = L_nT(i)$. 用同样的方法可以证明 $(Tq)_*\tau_A = L_nT(p)$. ■

系 10.55　*如果 $T: {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ 是加性共变函子，则函子 L_0T 是右正合的.*

证明　如果 $A \to B \to C \to 0$ 是正合的，则 $L_0A \to L_0B \to L_0C \to 0$ 也是正合的. ■

841

定理 10.56　（i）*如果一个加性共变函子 $T: {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ 是右正合的，则 T 和 L_0T 自然等价.*

（ii）*函子 $\otimes_R B$ 和 $\mathrm{Tor}_0^R(\ ,B)$ 自然等价. 因此对一切右 R-模 A，存在同构*

$$A \otimes_R B \cong \mathrm{Tor}_0^R(A,B).$$

⊖ 复形的正合列不是分裂的，因为分裂映射的序列未必组成链映射 $\mathbf{P}''_{A''} \to \widetilde{\mathbf{P}}_A$.

证明 （ⅰ）设 $\mathbf{P}_A$ 是 A 的选定的删除投射分解，并设

$$\cdots \to P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} A \to 0$$

是选定的投射分解．根据定义，

$$L_0 TA = \operatorname{coker} T(d_1).$$

但 T 的右正合性给出正合列

$$TP_1 \xrightarrow{Td_1} TP_0 \xrightarrow{T\varepsilon} TA \to 0.$$

现在根据第一同构定理，$T\varepsilon$ 诱导出一个同构 $\sigma_A : \operatorname{coker} T(d_1) \to TA$；即 $\sigma_A : L_0 TA \to TA$. $\sigma : L_0 T \to T$ 是自然等价的证明留作一个平淡的习题．

（ⅱ）从（ⅰ）立得，因为 $\otimes_R B$ 是右正合加性共变函子． ■

我们已经证明 Tor 修补了正合性的缺失，在对一个短正合列采用张量积之后可能产生这种缺失．

系 10.57 如果 $0 \to A' \to A \to A'' \to 0$ 是模的短正合列，则存在长正合列

$$\cdots \to \operatorname{Tor}_2^R(A',B) \to \operatorname{Tor}_2^R(A,B) \to \operatorname{Tor}_2^R(A'',B)$$
$$\to \operatorname{Tor}_1^R(A',B) \to \operatorname{Tor}_1^R(A,B) \to \operatorname{Tor}_1^R(A'',B)$$
$$\to A' \otimes_R B \to A \otimes_R B \to A'' \otimes_R B \to 0.$$

下一命题证明函子 $\operatorname{Tor}_n(\ ,B)$ 满足定理 10.45 共变形式．

命题 10.58 给定模的行正合的交换图，

$$\begin{array}{ccccccccc} 0 & \to & A' & \xrightarrow{i} & A & \xrightarrow{p} & A'' & \to & 0 \\ & & \downarrow{f} & & \downarrow{g} & & \downarrow{h} & & \\ 0 & \to & C' & \xrightarrow{j} & C & \xrightarrow{q} & C'' & \to & 0 \end{array}$$

842

对一切 n，存在行正合的交换图

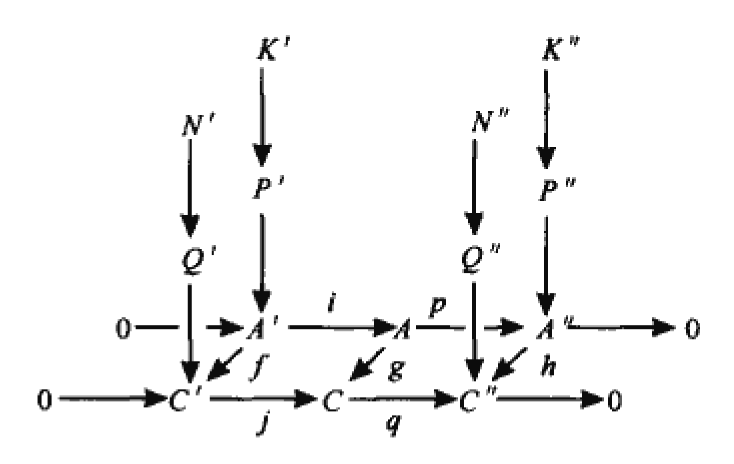
$$\begin{array}{ccccccc} \operatorname{Tor}_n^R(A',B) & \xrightarrow{i_*} & \operatorname{Tor}_n^R(A,B) & \xrightarrow{p_*} & \operatorname{Tor}_n^R(A'',B) & \xrightarrow{\partial_n} & \operatorname{Tor}_{n-1}^R(A',B) \\ \downarrow{f_*} & & \downarrow{g_*} & & \downarrow{h_*} & & \downarrow{f_*} \\ \operatorname{Tor}_n^R(C',B) & \xrightarrow{j_*} & \operatorname{Tor}_n^R(C,B) & \xrightarrow{q_*} & \operatorname{Tor}_n^R(C'',B) & \xrightarrow{\partial_n'} & \operatorname{Tor}_{n-1}^R(C',B) \end{array}$$

如果固定第一个变量，则有类似的图．

证明 给定陈述中的图，在交角上建立选定的删除投射分解 $\mathbf{P}'_{A'}$, $\mathbf{P}''_{A''}$, $\mathbf{Q}'_{C'}$ 和 $\mathbf{Q}''_{C''}$. 我们断言存在删除投射分解 $\widetilde{\mathbf{P}}_A$ 和 $\widetilde{\mathbf{Q}}_C$，它们和链映射一起给出复形的行正合的交换图：

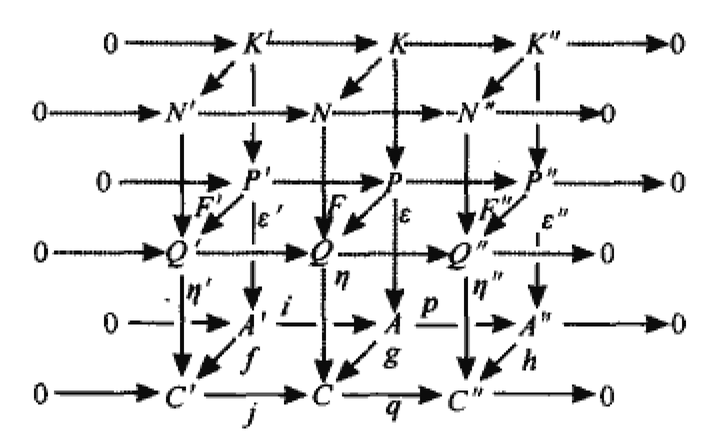
$$\begin{array}{ccccccccc} 0 & \to & \mathbf{P}'_{A'} & \xrightarrow{\check{i}} & \widetilde{\mathbf{P}}_A & \xrightarrow{\check{p}} & \mathbf{P}''_{A''} & \to & 0 \\ & & \downarrow{\check{f}} & & \downarrow{\check{g}} & & \downarrow{\check{h}} & & \\ 0 & \to & \mathbf{Q}'_{C'} & \xrightarrow{\check{j}} & \widetilde{\mathbf{Q}}_C & \xrightarrow{\check{q}} & \mathbf{Q}''_{C''} & \to & 0 \end{array}$$

一旦做好以后，由连接同态的自然性就可得到结果．和引理 10.53 的归纳证明一样，只需证明三维形式的蹄铁引理．下面的交换图中，列是短正合列，P', P'', Q' 和 Q'' 都是投射的，N', N'', K' 和 K'' 都是核．



843

我们用下面的图来完成这个图，下面的图中，行和列都是短正合列，P 和 Q 是投射的：



第 1 步．根据比较定理，存在 f 上的链映射 $\check{f}:\mathbf{P}'_{A'}\to\mathbf{Q}'_{C'}$ 和 h 上的链映射 $\check{h}:\mathbf{P}''_{A''}\to\mathbf{Q}''_{C''}$．为了简化记号，记 $F'=\check{f}_0$ 和 $F''=\check{h}_0$．

第 2 步．定义 $P=P'\oplus P''$，并插进通常的内射和投射映射 $P'\to P$ 和 $P\to P''$，即 $x'\mapsto(x',0)$ 和 $(x',x'')\mapsto x''$．类似地，定义 $Q=Q'\oplus Q''$，并插入内射和投射映射 $Q'\to Q$ 和 $Q\to Q''$．当然，序列 $0\to P'\to P\to P''\to 0$ 和 $0\to Q'\to Q\to Q''\to 0$ 都是正合的．

第 3 步．和蹄铁引理的证明一样，定义 $\varepsilon:P\to A$ 为 $\varepsilon:(x',x'')\mapsto i\varepsilon'x'+\sigma x''$，其中 $\sigma:P''\to A$ 满足 $p\sigma=\varepsilon''$（在蹄铁引理的证明中证明了存在这样的映射 σ）；事实上，蹄铁引理表明图的背面交换．类似地，定义 $\eta:Q\to C$ 为 $\eta:(y',y'')\mapsto j\eta'y'+\tau y''$，其中 $\tau:Q''\to C$ 满足 $q\tau=\eta''$；图的前面也交换．

第 4 步．定义 $F:P\to Q$ 为

$$F:(x',x'')\mapsto(F'x'+\gamma x'',F''x''),$$

其中 $\gamma:P''\to Q'$ 有待构造．易知，不管 γ 如何定义，包含各个 P 和各个 Q 的平面总是交换的．

第 5 步．剩下要选取 γ 使得有顶点 P，Q，C 和 A 的方块交换；即要使得 $g\varepsilon=\eta F$．两边赋值导出等式

$$gi\varepsilon'x'+g\sigma x''=j\eta'F'x'+j\eta'\gamma x''+\tau F''x''.$$

现在 $gi\varepsilon'=jf\varepsilon'=j\eta'F'$（因为 F' 是 f 上的链映射 $\check{f}$ 中的第 0 项），因此只需找到 γ 使得

844

$$j\eta'\gamma=g\sigma-\tau F''.$$

考虑行正合的图

$$\begin{array}{ccccc} & & P'' & & \\ & & \big\downarrow{\scriptstyle g\sigma-\tau F''} & & \\ Q' & \xrightarrow{j\eta'} & C & \xrightarrow{q} & C'' \end{array}$$

现在 $\mathrm{im}(g\sigma - \tau F'') \subseteq \mathrm{im}j\eta' = \ker q$，这是因为

$$qg\sigma - q\tau F'' = hp\sigma - \eta''F'' = h\varepsilon'' - \eta''F'' = 0.$$

因 P''是投射的，存在映射 $\gamma: P'' \to Q'$使得图交换．

第 6 步．根据 3×3 引理（习题 10.29），行 $0 \to K' \to K \to K'' \to 0$ 和 $0 \to N' \to N \to N'' \to 0$ 是正合的，我们让读者证明图的顶面存在映射使得每个方块交换． ■

下一节我们说明如何计算和使用 Tor. 但结束本节之前，和刚给出的对于张量积的处理一样，我们给出对于 Hom 的处理．

函子 T 的左导函子的定义要求 $T\mathbf{P}_A$ 是它的一切非零项都在左端的复形；即一切负次项都是 $\{0\}$. 这个定义的一个推论是系 10.55：如果 T 是右正合的，则 L_0T 和 T 自然等价．当 Hom 函子左正合时，用 $T\mathbf{C}$. 在右端的删除分解 $\mathbf{C}$. 来定义右导函子 R^nT. 我们将看到当 T 左正合时，R^0T 和 T 自然等价．

给定一个加性共变函子 $T: {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$，其中 R 和 S 是环，对一切 $n \in \mathbb{Z}$，我们构造它的**右导函子** $R^nT: {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$.

一次性地对每个模 A 选取一个删除内射分解 $\mathbf{E}^A$，形成复形 $T\mathbf{E}^A$，并取同调：

$$R^nT(A) = H^n(T\mathbf{E}^A) = \frac{\ker Td^n}{\mathrm{im}\, Td^{n-1}}.$$

读者应重温例10.34(X)以回忆指标约定为上升；如果指标下降，则定义会是

$$R^nT(A) = H_{-n}(T\mathbf{E}^A) = \frac{\ker Td_{-n}}{\mathrm{im}\, Td_{-n+1}}.$$

注意，我们曾在同调模上提升过指标；我们把 H_{-n} 写成 H^n．

$R^nT(f)$的定义（其中 $f: A \to A'$是同态）类似于左导函子的定义．根据比较定理的对偶定理，存在 f 上的链映射 $\check{f}: \mathbf{E}^A \to \mathbf{E}'A'$，且不计同伦是唯一的，因此在同调中诱导出唯一的映射 $R^nT(f): H^n(T\mathbf{E}^A) \to H^n(T\mathbf{E}'^{A'})$，就是 $(T\check{f}_n)_*$．

845

用图说明，考虑选定的内射分解：

$$\begin{array}{ccccccccc} 0 & \to & A' & \to & E'^0 & \to & E'^1 & \to & \cdots \\ & & f\uparrow & & & & & & \\ 0 & \to & A & \to & E^0 & \to & E^1 & \to & \cdots \end{array}$$

填入 f 上的链映射 $\check{f}$，然后对这个图运用 T，再取由 $T\check{f}$ 在同调中诱导的映射．

命题 10.59 给定一对环 R 和 S 以及一个加性共变函子 $T: {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$，则对每个 n，

$$R^nT: {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$$

是一个加性共变函子．

这个命题的证明和马上要陈述的关于右导函子的其他命题的证明本质上是我们已经给出的证明的对偶，因此省略．

例 10.60 如果 T 是一个保持乘法的加性共变函子，又如果 $\mu_r: A \to A$ 是乘 r，其中 $r \in Z(R)$是一个中心元素，则 R^nT 也保持乘法（见例 10.47）． ■

命题 10.61 如果 $T: {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ 是加性共变函子，则对一切负 n 和一切 A，$R^nTA = \{0\}$．

定义 如果 $T = \mathrm{Hom}_R(B, \ )$，定义 $\mathrm{Ext}_R^n(B, \ ) = R^nT$．于是，如果

$$\mathbf{E}^A = 0 \to E^0 \xrightarrow{d^0} E^1 \xrightarrow{d^1} E^2 \to \cdots$$

是模 A 的选定的删除内射分解，则

$$\mathrm{Ext}_R^n(B,A) = H^n(\mathrm{Hom}_R(B,\mathbf{E}^A)) = \frac{\ker(d^n)_*}{\mathrm{im}(d^{n-1})_*},$$

其中 $(d^n)_* : \mathrm{Hom}_R(B,E^n) \to \mathrm{Hom}_R(B,E^{n+1})$ 和通常一样定义为

$$(d^n)_* : f \mapsto d^n f.$$

R^nT 的定义域，特别是 $\mathrm{Ext}_R^n(B,\ )$ 的定义域是 ${}_R\mathbf{Mod}$，它是一切左 R-模的范畴，其目标域是 **Ab**，是阿贝尔群的范畴．目标域可以较大；例如，当 R 交换时，它是 ${}_R\mathbf{Mod}$.

假定选取了新的删除内射分解 $\widetilde{\mathbf{E}}^A$，我们记由这些新的选取形成的右导函子为 $\widetilde{R}^nT$.

846

命题 10.62　给定一对环 R 和 S 以及一个加性共变函子 $T: {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$，则对每个 n，函子 R^nT 和 $\widetilde{R}^nT$ 自然等价．特别地，对一切 A，

$$(R^nT)A \cong (\widetilde{R}^nT)A,$$

从而这些模不依赖于 A 的（删除）内射分解的选取．

系 10.63　模 $\mathrm{Ext}_R^n(B,A)$ 不依赖于 A 的内射分解的选取．

系 10.64　设 $T: {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ 是一个加性共变函子．如果 E 是一个内射模，则对一切 $n \geqslant 1$，$R^nT(E) = \{0\}$．

特别地，如果 E 是一个内射 R-模，则对一切 $n \geqslant 1$ 和一切模 B，$\mathrm{Ext}_R^n(B,E) = \{0\}$．

定理 10.65　如果 $0 \to A' \xrightarrow{i} A \xrightarrow{p} A'' \to 0$ 是模的正合列，又如果 $T: {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ 是一个加性共变函子，则存在长正合列：

$$\cdots \to R^nTA' \xrightarrow{R^nTi} R^nTA \xrightarrow{R^nTp} R^nTA'' \xrightarrow{\partial^n}$$
$$R^{n+1}TA' \xrightarrow{R^{n+1}Ti} R^{n+1}TA \xrightarrow{R^{n+1}Tp} R^{n+1}TA'' \xrightarrow{\partial^{n+1}} \cdots$$

它以

$$0 \to R^0TA' \to R^0TA \to R^0TA'' \to \cdots$$

起首．

系 10.66　如果 $T: {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ 是一个加性共变函子，则函子 R^0T 是左正合的．

定理 10.67　（i）如果加性共变函子 $T: {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ 是左正合的，则 T 和 R^0T 自然等价．

（ii）如果 B 是左 R-模，函子 $\mathrm{Hom}_R(B,\ )$ 和 $\mathrm{Ext}_R^0(B,\ )$ 自然等价．因此，对一切左 R-模 A，存在同构

$$\mathrm{Hom}_R(B,A) \cong \mathrm{Ext}_R^0(B,A).$$

我们已经证明 Ext 修补了正合性的缺失，它可能出现在对短正合列运用 Hom 之后．

847

系 10.68　如果 $0 \to A' \to A \to A'' \to 0$ 是模的短正合列，则存在长正合列

$$0 \to \mathrm{Hom}_R(B,A') \to \mathrm{Hom}_R(B,A) \to \mathrm{Hom}_R(B,A'')$$
$$\to \mathrm{Ext}_R^1(B,A') \to \mathrm{Ext}_R^1(B,A) \to \mathrm{Ext}_R^1(B,A'')$$
$$\to \mathrm{Ext}_R^2(B,A') \to \mathrm{Ext}_R^2(B,A) \to \mathrm{Ext}_R^2(B,A'') \to \cdots.$$

命题 10.69 给定模的行正合的交换图，

$$\begin{array}{ccccccccc} 0 & \to & A' & \xrightarrow{i} & A & \xrightarrow{p} & A'' & \to & 0 \\ & & \downarrow f & & \downarrow g & & \downarrow h & & \\ 0 & \to & C' & \xrightarrow{j} & C & \xrightarrow{q} & C'' & \to & 0 \end{array}$$

对一切 n，存在行正合的交换图

$$\begin{array}{ccccccc} \mathrm{Ext}_R^n(B,A') & \xrightarrow{i_*} & \mathrm{Ext}_R^n(B,A) & \xrightarrow{p_*} & \mathrm{Ext}_R^n(B,A'') & \xrightarrow{\partial^n} & \mathrm{Ext}_R^{n+1}(B,A') \\ \downarrow f_* & & \downarrow g_* & & \downarrow h_* & & \downarrow f_* \\ \mathrm{Ext}_R^n(B,C') & \xrightarrow{j_*} & \mathrm{Ext}_R^n(B,C) & \xrightarrow{q_*} & \mathrm{Ext}_R^n(B,C'') & \xrightarrow{\partial^n} & \mathrm{Ext}_R^{n+1}(B,C') \end{array}$$

最后，我们讨论反变函子 T 的导函子．如果用 $T\mathbf{C}_\bullet$ 在右端的删除分解 $\mathbf{C}_\bullet$ 来定义右导函子 R^nT，则从一个删除投射分解 $\mathbf{P}_A$ 出发，然后由 T 的反变性把 $T\mathbf{P}_A$ 放在右端．[⊖]

给定加性反变函子 $T:{}_R\mathbf{Mod}\to{}_S\mathbf{Mod}$，其中 R 和 S 都是环，现在对 $n\in\mathbb{Z}$ 构造它的右导函子 $R^nT:{}_R\mathbf{Mod}\to{}_S\mathbf{Mod}$.

一次性地对每个模 A 选取一个删除投射分解，形成复形 $T\mathbf{P}_A$，并取同调：

$$R^nT(A)=H^n(T\mathbf{P}_A)=\frac{\ker Td_{n+1}}{\operatorname{im} Td_n}.$$

如果 $f:A\to A'$，和对左导函子一样，定义 $R^nT(f):R^nT(A')\to R^nT(A)$．根据比较定理，存在 f 上的链映射 $\check{f}:\mathbf{P}_A\to\mathbf{P}'_{A'}$ 不计同伦是唯一的，它在同调中诱导出映射 $R^nT(f):H^n(T\mathbf{P}'_{A'})\to$

848

$H^n(T\mathbf{P}_A)$，就是 $(T\check{f}_n)_*$．

例 10.70 如果 T 是保持乘法的加性反变函子，又如果 $\mu_r:A\to A$ 是乘 r，其中 $r\in Z(R)$ 是中心元素，则 R^nT 也保持乘法（见例 10.47）． ■

命题 10.71 给定一对环 R 和 S 以及一个加性反变函子 $T:{}_R\mathbf{Mod}\to{}_S\mathbf{Mod}$，则对每个 n，

$$R^nT:{}_R\mathbf{Mod}\to{}_S\mathbf{Mod}$$

是一个加性反变函子.

命题 10.72 如果 $T:{}_R\mathbf{Mod}\to{}_S\mathbf{Mod}$ 是加性反变函子，则对一切负 n 和一切 A，$R^nTA=\{0\}$．

定义 如果 $T=\mathrm{Hom}_R(\ ,C)$，定义 $\mathrm{ext}_R^n(\ ,C)=R^nT$．于是，如果

$$\cdots\to P_2\xrightarrow{d_2}P_1\xrightarrow{d_1}P_0\to 0$$

是模 A 的选定的删除投射分解，则

$$\mathrm{ext}_R^n(A,C)=H^n\mathrm{Hom}_R(\mathbf{P}_A,C)=\frac{\ker(d_{n+1})^*}{\operatorname{im}(d_n)^*},$$

其中 $(d^n)^*:\mathrm{Hom}_R(P_{n-1},C)\to\mathrm{Hom}_R(P_n,C)$ 和通常一样定义为

$$(d_n)^*:f\mapsto fd_n.$$

对 Tor 成立的现象对 Ext 也成立：对一切 A 和 C（和对一切 R 和 n），

$$\mathrm{Ext}_R^n(A,C)\cong\mathrm{ext}_R^n(A,C).$$

对于 Tor 不依赖于变量分解的证明也适用于 Ext（见 Rotman 所著的《An Introduction to Homologi-

---

⊖ 如果我们对反变函子 T 的左导函子感兴趣（但我们对其不感兴趣），则用内射分解．

cal Algebra》, 197 页）. 根据这个定理，对 Ext 不必使用两个记号.

假定选取了新的删除投射分解 $\widetilde{\mathbf{P}}_A$，我们记这个新的选取形成的右导函子为 $\widetilde{R}^nT$.

命题 10.73 给定一对环 R 和 S 以及一个加性反变函子 $T: {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$，则对每个 n，函子 R^nT 和 $\widetilde{R}^nT$ 自然等价. 特别地，对一切 A，

$$(R^nT)A \cong (\widetilde{R}^nT)A,$$

849

从而这些模不依赖于 A 的（删除）投射分解的选取.

系 10.74 模 $\mathrm{Ext}_R^n(A,C)$ 不依赖于 A 的投射分解的选取.

系 10.75 设 $T: {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ 是加性反变函子. 如果 P 是一个投射模，则对一切 $n \geq 1$，$R^nT(P) = \{0\}$.

特别地，如果 P 是一个投射 R-模，则对一切 $n \geq 1$ 和一切模 B，$\mathrm{Ext}_R^n(P,B) = \{0\}$.

定理 10.76 如果 $0 \to A' \xrightarrow{i} A \xrightarrow{p} A'' \to 0$ 是模的正合列，又如果 $T: {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ 是加性反变函子，则存在长正合列

$$\cdots \to R^nTA'' \xrightarrow{R^nTp} R^nTA \xrightarrow{R^nTi} R^nTA' \xrightarrow{\partial^n}$$
$$R^{n+1}TA'' \xrightarrow{R^{n+1}Tp} R^{n+1}TA \xrightarrow{R^{n+1}Ti} R^{n+1}TA' \xrightarrow{\partial^{n+1}} \cdots$$

它以

$$0 \to R^0TA'' \to R^0TA \to R^0TA' \to \cdots$$

开头.

系 10.77 如果 $T: {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ 是加性反变函子，则函子 R^0T 是左正合的.

定理 10.78 （i）如果一个加性反变函子 $T: {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ 是左正合的，则 T 和 R^0T 自然等价.

（ii）如果 C 是一个左 R-模，函子 $\mathrm{Hom}_R(\ ,C)$ 和 $\mathrm{Ext}_R^0(\ ,C)$ 自然等价. 因此，对一切左 R-模 A，存在同构

$$\mathrm{Hom}_R(A,C) \cong \mathrm{Ext}_R^0(A,C).$$

我们已经证明 Ext 修补了正合性的缺失，它可能出现在对一个短正合列运用 Hom 之后.

系 10.79 如果 $0 \to A' \to A \to A'' \to 0$ 是模的短正合列，则存在长正合列

$$0 \to \mathrm{Hom}_R(A'',C) \to \mathrm{Hom}_R(A,C) \to \mathrm{Hom}_R(A',C)$$
$$\to \mathrm{Ext}_R^1(A'',C) \to \mathrm{Ext}_R^1(A,C) \to \mathrm{Ext}_R^1(A',C)$$
$$\to \mathrm{Ext}_R^2(A'',C) \to \mathrm{Ext}_R^2(A,C) \to \mathrm{Ext}_R^2(A',C) \to \cdots.$$

850

命题 10.80 给定模的行正合的交换图，

$$\begin{array}{ccccccccc} 0 & \to & A' & \xrightarrow{i} & A & \xrightarrow{p} & A'' & \to & 0 \\ & & \downarrow f & & \downarrow g & & \downarrow h & & \\ 0 & \to & C' & \xrightarrow{j} & C & \xrightarrow{q} & C'' & \to & 0 \end{array}$$

对一切 n，存在行正合的交换图

$$\begin{array}{ccccccc} \mathrm{Ext}_R^n(A'',B) & \xrightarrow{p^*} & \mathrm{Ext}_R^n(A,B) & \xrightarrow{i^*} & \mathrm{Ext}_R^n(A',B) & \xrightarrow{\partial^n} & \mathrm{Ext}_R^{n+1}(A'',B) \\ \uparrow h^* & & \uparrow g^* & & \uparrow f^* & & \uparrow h^* \\ \mathrm{Ext}_R^n(C'',B) & \xrightarrow{q^*} & \mathrm{Ext}_R^n(C,B) & \xrightarrow{j^*} & \mathrm{Ext}_R^n(C',B) & \xrightarrow{\partial^{n\prime}} & \mathrm{Ext}_R^{n+1}(C'',B) \end{array}$$

注 当 T 是共变函子时，我们称 L_nT 的要素为链、圈、边界和同调．当 T 是反变函子时，我们常加一前缀"上"，R^nT 的要素常称为上链、余圈、上边界和上同调．不幸的是这个清楚的区分是模糊的，因为 Hom 函子在一个变量中是反变的，而在另一个变量中是共变的．尽管如此，对 Hom 的导函子 Ext^n 我们还是常用前缀"上"．

导函子是构造诸如 Ext 和 Tor 的共变函子的一种方法．在下节中，我们将给出 Ext 与 Tor 的更多性质，并将描述属于米田信夫（N. Yoneda）的关于 Ext 的另一种构造和属于麦克莱恩的关于 Tor 的另一种构造，其实，导函子在后面是很少提及的．

习题

10.36 如果 $F \to G$ 是加性函子之间的自然变换，证明对每个复形 $\mathbf{C}$，τ 给出链映射 $\tau_{\mathbf{C}}: F\mathbf{C} \to G\mathbf{C}$. 如果 τ 是自然等价，证明 $F\mathbf{C} \cong G\mathbf{C}$.

10.37 （ⅰ）设 $T: {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ 是正合加性函子，其中 R 和 S 是环，并假定 P 投射蕴涵 TP 投射．如果 B 是左 R-模，$\mathbf{P}_B$ 是 B 的删除投射分解，证明 $T\mathbf{P}_{TB}$ 是 TB 的删除投射分解．

（ⅱ）设 A 是 R-代数且作为 R-模是平坦的，其中 R 是交换环．证明：如果 B 是 A-模（因此是 R-模），则对一切 R-模 C 和一切 $n \geqslant 0$，

851

$$A \otimes_R \text{Tor}_n^R(B,C) \cong \text{Tor}_n^A(B, A \otimes_R C).$$

10.38 设 R 是半单环．

（ⅰ）证明对一切 $n \geqslant 1$，对一切右 R-模 A 和一切左 R-模 B 有 $\text{Tor}_n^R(A,B) = \{0\}$.

提示：如果 R 是半单的，则每个（左或右）R-模是投射的．

（ⅱ）证明对一切 $n \geqslant 1$，对一切左 R-模 A 和 B 有 $\text{Ext}_R^n(A,B) = \{0\}$.

10.39 如果 R 是 PID，证明对一切 $n \geqslant 2$，对一切 R-模 A 和 B 有 $\text{Tor}_n^R(A,B) = \{0\} = \text{Ext}_R^n(A,B)$.

提示：用定理 9.8.

10.40 设 R 是整环并设 A 是 R-模．

（ⅰ）证明：如果对一切 $r \neq 0$，乘映射 $\mu_r: A \to A$ 是单射，则 A 是无挠的．

（ⅱ）证明：如果对一切 $r \neq 0$，乘映射 $\mu_r: A \to A$ 是满射，则 A 是可除的．

（ⅲ）证明：如果对一切 $r \neq 0$，乘映射 $\mu_r: A \to A$ 是同构，则 A 是 Q 上的向量空间，其中 $Q = \text{Frac}(R)$.

提示：模 A 是 Q 上的向量空间当且仅当它是无挠的和可除的．

（ⅳ）如果 C 或者 A 是 Q 上的向量空间，证明 $\text{Tor}_n^R(C,A)$ 和 $\text{Ext}_R^n(C,A)$ 也是 Q 上的向量空间．

10.41 设 R 是整环并设 $Q = \text{Frac}(R)$.

（ⅰ）如果 $r \in R$ 是非零元素且 A 是满足 $rA = \{0\}$ 的 R-模，即对一切 $a \in A$，$ra = 0$，证明对一切 $n \geqslant 0$，$\text{Ext}_R^n(Q,A) = \{0\} = \text{Tor}_n^R(Q,A)$.

提示：如果 V 是 Q 上的向量空间满足 $rV = \{0\}$，则 $V = \{0\}$.

（ⅱ）证明对一切 $n \geqslant 0$，只要 V 是 Q 上的向量空间且 A 是有某个非零 $r \in R$ 使得 $rA = \{0\}$ 的 R-模，就有 $\text{Ext}_R^n(V,A) = \{0\} = \text{Tor}_n^R(V,A)$.

10.42 设 A 和 B 都是 R-模．对 $f: A' \to B$，其中 A' 是 A 的子模，定义它的障碍为 $\partial(f)$，其中 $\partial: \text{Hom}_R(A',B) \to \text{Ext}_R^1(A/A',B)$ 是连接同态．证明 f 能够扩张为同态 $\tilde{f}: A \to B$ 当且仅当它的障碍是 0.

10.43 如果 $T: \mathbf{Ab} \to \mathbf{Ab}$ 是左正合函子，证明 L_0T 是正合函子．由此推出，对任意阿贝尔群 B，$L_0\text{Hom}(B, \ )$ 和 $\text{Hom}(B, \ )$ 不自然等价．

10.6 Ext 和 Tor

我们现在更仔细地考察 Ext 和 Tor. 上节说过,这两个函子的一切性质可以从定理 10.45 的版本中得到,这个定理是刻画它们的公理(见习题 10.44 和 10.45);特别地,不必把它们作为导函子来构造.

我们先证明 Ext 关于和与积具有与 Hom 类似的性态. [852]

命题 10.81 *如果 $\{A_k : k\in K\}$ 是模的族,则对一切 n,存在自然同构,*

$$\mathrm{Ext}_R^n\Big(\sum_{k\in K}A_k,\ B\Big)\cong\prod_{k\in K}\mathrm{Ext}_R^n\ (A_k,B).$$

证明 用长度推移法进行证明;即对 $n\geqslant 0$ 用归纳法. 基础步是定理 7.33,这是因为 $\mathrm{Ext}^0(\ \ ,B)$ 和反变函子 $\mathrm{Hom}(\ \ ,B)$ 自然等价.

关于归纳步,对每个 $k\in K$ 选取一个短正合列

$$0\to L_k\to P_k\to A_k\to 0,$$

其中 P_k 是投射模. 存在正合列

$$0\to\sum_k L_k\to\sum_k P_k\to\sum_k A_k\to 0,$$

因为投射模的和也是投射模,所以 $\sum\limits_k P_k$ 是投射模. 存在行正合的交换图:

$$\begin{array}{ccccccc}
\mathrm{Hom}(\sum P_k,B) & \longrightarrow & \mathrm{Hom}(\sum L_k,B) & \xrightarrow{\partial} & \mathrm{Ext}^1(\sum A_k,B) & \longrightarrow & \mathrm{Ext}^1(\sum P_k,B)\\
\downarrow{\scriptstyle\tau} & & \downarrow{\scriptstyle\sigma} & & \vdots & & \\
\prod\mathrm{Hom}(P_k,B) & \longrightarrow & \prod\mathrm{Hom}(L_k,B) & \xrightarrow{d} & \prod\mathrm{Ext}^1(A_k,B) & \longrightarrow & \prod\mathrm{Ext}^1(P_k,B)
\end{array}$$

其中底下一行的映射在每个坐标中恰是通常的诱导映射,映射 τ 和 σ 是定理 7.33 给出的同构. 现在 $\mathrm{Ext}^1(\sum P_k,B)=\{0\}=\prod\mathrm{Ext}^1(P_k,B)$,这是因为 $\sum P_k$ 和每个 P_k 都是投射的,从而映射 ∂ 和 d 都是满射. 这就是命题 8.93 中的那种图,因此存在同构 $\mathrm{Ext}^1(\sum A_k,B)\to\prod\mathrm{Ext}^1(A_k,B)$ 使得增广的图交换.

现在可以假定 $n\geqslant 1$,并进一步注意长正合列. 存在交换图

$$\begin{array}{ccccccc}
\mathrm{Ext}^n(\sum P_k,B) & \longrightarrow & \mathrm{Ext}^n(\sum L_k,B) & \xrightarrow{\partial} & \mathrm{Ext}^{n+1}(\sum A_k,B) & \longrightarrow & \mathrm{Ext}^{n+1}(\sum P_k,B)\\
 & & \downarrow{\scriptstyle\sigma} & & \vdots & & \\
\prod\mathrm{Ext}^n(P_k,B) & \longrightarrow & \prod\mathrm{Ext}^n(L_k,B) & \xrightarrow{d} & \prod\mathrm{Ext}^{n+1}(A_k,B) & \longrightarrow & \prod\mathrm{Ext}^{n+1}(P_k,B)
\end{array}$$

其中 $\sigma:\mathrm{Ext}^n(\sum L_k,B)\to\prod\mathrm{Ext}^n(L_k,B)$ 是同构,根据归纳假设它是存在的. 因 $n\geqslant 1$,第一个变量是投射的四个 Ext 都是 $\{0\}$;由此,根据行的正合性可知 ∂ 和 d 都是同构. 最后,正如所要的,复合 $d\sigma\partial^{-1}:\mathrm{Ext}^{n+1}(\sum A_k,B)\to\prod\mathrm{Ext}^{n+1}(A_k,B)$ 是同构. ■

对第二个变量有一个对偶结果. [853]

命题 10.82 *如果 $\{B_k : k\in K\}$ 是模的族,则对一切 n,存在自然同构,*

$$\mathrm{Ext}_R^n\Big(A,\prod_{k\in K}B_k\Big)\cong\prod_{k\in K}\mathrm{Ext}_R^n(A,B_k).$$

证明 用长度推移法进行证明. 基础步是定理 7.32,这是因为 $\mathrm{Ext}^0(A,\ )$ 和共变函子 $\mathrm{Hom}(A,\ )$ 自然等价.

关于归纳步,对每个 $k\in K$ 选取一个短正合列

$$0\to B_k\to E_k\to N_k\to 0,$$

其中 E_k 是内射模. 存在正合列

$$0 \to \prod_k B_k \to \prod_k E_k \to \prod_k N_k \to 0,$$

因为根据命题 7.66，内射模的积也是内射模，所以 $\prod_k E_k$ 是内射模. 存在行正合的交换图：

$$\begin{array}{ccccccc}
\mathrm{Hom}(A, \prod E_k) & \to & \mathrm{Hom}(A, \prod N_k) & \xrightarrow{\partial} & \mathrm{Ext}^1(A, \prod B_k) & \to & \mathrm{Ext}^1(A, \prod E_k) \\
\downarrow \tau & & \downarrow \sigma & & \downarrow & & \\
\prod \mathrm{Hom}(A, E_k) & \to & \prod \mathrm{Hom}(A, N_k) & \xrightarrow{d} & \prod \mathrm{Ext}^1(A, B_k) & \to & \prod \mathrm{Ext}^1(A, E_k)
\end{array}$$

其中底下一行的映射在每个坐标中恰是通常的诱导映射，映射 τ 和 σ 是定理 7.32 给出的同构. 现在证明可以如同命题 10.81 那样完成. ■

由此无论对那个变量，Ext^n 与有限直和交换.

注 上面两个命题不能够把和替换为正向极限，或把积替换为反向极限而加以推广；理由是投射模的正向极限未必是投射的，和内射模的反向极限未必是内射的.

当环 R 非交换时，$\mathrm{Hom}_R(A,B)$是阿贝尔群，但它未必是 R-模.

命题 10.83 （i） $\mathrm{Ext}^n_R(A,B)$ 是 $Z(R)$-模. 特别地，如果 R 是交换环，则 $\mathrm{Ext}^n_R(A,B)$ 是R-模.

（ii） 如果 A 和 B 都是左 R-模且 $r \in Z(R)$ 是中心元素，$\mu_r: B \to B$ 是乘 r 的映射，则诱导映射 μ_r^*：$\mathrm{Ext}^n_R(A,B) \to \mathrm{Ext}^n_R(A,B)$ 也是乘 r 的映射. 类似陈述对另一个变量也成立.

证明 （i）由例 10.47，μ_r 是 R-映射，因此它诱导出 $\mathrm{Ext}^n_R(A,B)$ 上的一个同态. 容易验证 $x \mapsto \mu_r^*(x)$ 定义了一个标量乘法 $Z(R) \times \mathrm{Ext}^n_R(A,B) \to \mathrm{Ext}^n_R(A,B)$.

854

（ii）因为我们定义乘标量 r 的映射为 μ_r^*，则由（i）可得结果. ■

例 10.84 （i）我们证明对阿贝尔群 B 有

$$\mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{I}_n, B) \cong B/nB.$$

存在正合列

$$0 \to \mathbb{Z} \xrightarrow{\mu_n} \mathbb{Z} \to \mathbb{I}_n \to 0,$$

其中 μ_n 是乘 n. 运用 $\mathrm{Hom}(\ ,B)$得

$$\mathrm{Hom}(\mathbb{Z}, B) \xrightarrow{\mu_n^*} \mathrm{Hom}(\mathbb{Z}, B) \to \mathrm{Ext}^1(\mathbb{I}_n, B) \to \mathrm{Ext}^1(\mathbb{Z}, B)$$

的正合性. 现在因为 $\mathbb{Z}$ 是投射的，所以 $\mathrm{Ext}^1(\mathbb{Z}, B) = \{0\}$. 此外，$\mu_n^*$ 也是乘 n，而 $\mathrm{Hom}(\mathbb{Z}, B) = B$. 更精确地说，$\mathrm{Hom}(\mathbb{Z},\ )$ 和 **Ab** 上的单位函子自然等价，因此存在行正合的交换图

$$\begin{array}{ccccccc}
B & \xrightarrow{\mu_n} & B & \to & B/nB & \to & 0 \\
\downarrow \tau_B & & \downarrow \tau_B & & \downarrow & & \\
\mathrm{Hom}(\mathbb{Z},B) & \xrightarrow{\mu_n^*} & \mathrm{Hom}(\mathbb{Z},B) & \to & \mathrm{Ext}^1(\mathbb{I}_n,B) & \to & 0
\end{array}$$

根据命题 8.93，存在同构 $B/nB \cong \mathrm{Ext}^1(\mathbb{I}_n, B)$.

（ii）现在只要 A 和 B 都是有限生成的阿贝尔群，我们就能够计算 $\mathrm{Ext}^1_{\mathbb{Z}}(A,B)$. 根据基本定理，$A$ 和 B 都是循环群的直和. 因 Ext 与有限直和交换，$\mathrm{Ext}^1_{\mathbb{Z}}(A,B)$ 是群 $\mathrm{Ext}^1_{\mathbb{Z}}(C,D)$ 的直和，其中 C 和 D 都是循环群. 我们可以假定 C 是有限的，否则它是投射的，从而 $\mathrm{Ext}^1(C,D) = \{0\}$. 这个计算可以用

(i) 和习题 5.5 完成，它说如果 D 是有有限阶 m 的循环群，则 D/nD 是 d 阶循环群，其中 $d=(m,n)$ 是它们的 gcd. ■

我们现在给出类似于群扩张的显而易见的定义.

定义 给定 R-模 C 和 A，A 和 C 的一个**扩张**是指一个短正合列

$$0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0.$$

如果存在 R-映射 $s: C \to B$ 使得 $ps = 1_C$，则称这个扩张是**分裂**的.

当然，如果 $0 \to A \to B \to C \to 0$ 是分裂扩张，则 $B \cong A \oplus C$.

只要遇到同调群，我们必然要问它是零意味着什么，因为它的元素能够构造成为障碍物. 例如，因子组说明一个群扩张为什么不分裂. 本节中，我们将证明 $\mathrm{Ext}_R^1(C,A)=\{0\}$ 当且仅当 A 和 C 的每一个扩张分裂. 于是，任意 $\mathrm{Ext}_R^1(C',A')$ 的非零元素描述非分裂扩张（其实，这个结果是名称 Ext 的由来）.

855

我们从命题 10.17 引发的一个定义开始.

定义 给定模 C 和 A，如果对 A 和 C 的两个扩张 $\xi: 0 \to A \to B \to C \to 0$ 和 $\xi': 0 \to A \to B' \to C \to 0$，存在映射 $\varphi: B \to B'$ 使得下图交换：

$$\begin{array}{lcccccccc}
\xi: & 0 & \longrightarrow & A & \xrightarrow{i} & B & \xrightarrow{p} & C & \longrightarrow 1 \\
 & & & \downarrow{\scriptstyle 1_A} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle 1_C} & \\
\xi': & 0 & \longrightarrow & A & \xrightarrow{i'} & B' & \xrightarrow{p'} & C & \longrightarrow 1
\end{array}$$

则称这两个扩张**等价**. 我们记一个扩张 ξ 的等价类为 $[\xi]$，并记

$$e(C,A) = \{[\xi] : \xi \text{ 是 } A \text{ 和 } C \text{ 的扩张}\}.$$

如果两个扩张等价，则五项引理（习题 8.52）表明映射 φ 必是同构；由此等价实际上是一个等价关系（因为现在可以证明对称性）. 然而，反过来不成立：如同在例 10.18 中看到的（这个例中的一切群都是阿贝尔群，因此可以把它看作 $\mathbb{Z}$-模的例子），可以有中间项同构的不等价的扩张.

命题 10.85 如果 $\mathrm{Ext}_R^1(C,A)=\{0\}$，则每个扩张

$$0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$$

是分裂的.

证明 运用函子 $\mathrm{Hom}(C,\ )$ 到这个扩张上得到正合列

$$\mathrm{Hom}(C,B) \xrightarrow{p_*} \mathrm{Hom}(C,C) \xrightarrow{\partial} \mathrm{Ext}^1(C,A).$$

根据假设，$\mathrm{Ext}^1(C,A)=\{0\}$，从而 p_* 是满射. 因此，存在 $s \in \mathrm{Hom}(C,B)$ 使得 $1_C = p_*(s)$；即 $1_C = ps$，这就是说扩张分裂. ■

系 10.86 R-模 P 是投射的当且仅当对每个 R-模 B，$\mathrm{Ext}_R^1(P,B)=\{0\}$.

证明 如果 P 是投射的，则根据系 10.75，对一切 B，$\mathrm{Ext}_R^1(P,B)=\{0\}$. 反之，如果对一切 B，$\mathrm{Ext}_R^1(P,B)=\{0\}$，则根据命题 10.85，每个正合列 $0 \to B \to X \to P \to 0$ 分裂，因此根据命题 7.54，P 是投射的. ■

我们将通过证明存在双射 $\psi: e(C,A) \to \mathrm{Ext}^1(C,A)$ 来证明命题 10.85 的逆. 现在构造函数 ψ.

给定扩张 $\xi: 0 \to A \to B \to C \to 0$ 和 C 的投射分解，形成图

$$\begin{array}{ccccccccc} P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} & P_0 & \longrightarrow & C & \longrightarrow & 0 \\ \downarrow & & \downarrow \alpha & & \downarrow & & \downarrow 1_C & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \end{array}$$

856

根据比较定理（定理 10.46），可以填入虚线箭头得到一个交换图．特别地，存在映射 $\alpha: P_1 \to A$ 使得 $\alpha d_2 = 0$；即 $d_2^*(\alpha) = 0$，从而 $\alpha \in \ker d_2^*$ 是余圈．比较定理还说，图中的任意两个填充同伦；于是，如果 $\alpha': P_1 \to A$ 是第二个填充的一部分，则存在映射 s_0 和 s_1 使得 $\alpha' - \alpha = 0 \cdot s_1 + s_0 d_1 = s_0 d_1$：

$$\begin{array}{ccccc} P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} & P_0 \\ & \swarrow s_1 & \alpha' \downarrow\downarrow \alpha & \swarrow s_0 & \\ 0 & \longrightarrow & A & \longrightarrow & B \end{array}$$

从而 $\alpha' - \alpha \in \mathrm{im} d_1^*$，因此同调类 $\alpha + \mathrm{im} d_1^* \in \mathrm{Ext}^1(C, A)$ 是合理定义的．作为习题我们留给读者证明等价扩张 ξ 和 ξ' 确定的 Ext 的元素相同．于是由

$$\psi([\xi]) = \alpha + \mathrm{im}\ d_1^*$$

给出的

$$\psi: e(C, A) \to \mathrm{Ext}^1(C, A)$$

是合理定义的函数．注意，如果 ξ 上有分裂扩张，则 $\psi([\xi]) = 0$. 为了证明 ψ 是双射，我们先分析含有映射 α 的图.

引理 10.87 设 $\Xi: 0 \to X_1 \xrightarrow{j} X_0 \xrightarrow{\varepsilon} C \to 0$ 是模 X_1 和模 C 的一个扩张．给定模 A，考虑图

$$\begin{array}{ccccccccc} \Xi: 0 & \longrightarrow & X_1 & \xrightarrow{j} & X_0 & \xrightarrow{\varepsilon} & C & \longrightarrow & 0 \\ & & \downarrow \alpha & & & & \downarrow 1_C & & \\ & & A & & & & C & & \end{array}$$

（ⅰ）存在行正合的交换图完成这个给定的图：

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X_1 & \xrightarrow{j} & X_0 & \xrightarrow{\varepsilon} & C & \longrightarrow & 0. \\ & & \downarrow \alpha & & \downarrow \beta & & \downarrow 1_C & & \\ 0 & \longrightarrow & A & \xrightarrow{i} & B & \xrightarrow{\eta} & C & \longrightarrow & 0 \end{array}$$

（ⅱ）任意两个完成的图的底下一行是等价扩张．

证明 （ⅰ）我们定义 B 为 j 和 α 的推出．于是，如果

857

$$S = \{(\alpha x_1, -j x_1) \in A \oplus X_0 : x_1 \in X_1\},$$

定义 $B = (A \oplus X_0)/S$，

$$i: a \mapsto (a, 0) + S, \beta: x_0 \mapsto (0, x_0) + S, \eta: (a, x_0) + S \mapsto \varepsilon x_0 .$$

留给读者验证 η 是合理定义的、图交换和底下一行是正合的．

（ⅱ）设

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X_1 & \xrightarrow{j} & X_0 & \xrightarrow{\varepsilon} & C & \longrightarrow & 0. \\ & & \downarrow \alpha & & \downarrow \beta' & & \downarrow 1_C & & \\ 0 & \longrightarrow & A & \xrightarrow{i'} & B' & \xrightarrow{\eta'} & C & \longrightarrow & 0 \end{array}$$

是图的第二个完备化．定义 $f: A \oplus X_0 \to B'$ 为

$$f: (a, x_0) \mapsto i'a + \beta' x_0 .$$

我们断言 f 是满射．如果 $b' \in B'$，则 $\eta' b' \in C$，因此存在 $x_0 \in X_0$ 使得 $\varepsilon x_0 = \eta' b'$．交换性给出 $\eta' \beta' x_0 = \varepsilon x_0 = \eta' b'$．因此 $b' - \beta' x_0 \in \ker \eta' = \mathrm{im} i'$，从而有 $a \in A$ 使得 $i'a = b' - \beta' x_0$．所以正如所要的，

$b' = i'a + \beta' x_0 \in \operatorname{im} f$.

我们现在证明 $\ker f = S$．如果 $(\alpha x_1, -jx_1) \in S$，则根据这个图的第一个方块的交换性，$f(\alpha x_1, -jx_1) = i'\alpha x_1 - \beta' j x_1 = 0$，因此 $S \subseteq \ker f$．关于反包含，设$(a, x_0) \in \ker f$，从而 $i'a + \beta' x_0 = 0$．第二个方块的交换性给出 $\varepsilon x_0 = \eta' \beta' x_0 = -\eta' i' a = 0$．因此 $x_0 \in \ker \varepsilon = \operatorname{im} j$，从而存在 $x_1 \in X_1$ 使得 $jx_1 = x_0$ 于是，$i'a = -\beta' x_0 = -\beta' j x_1 = -i'\alpha x_1$．因 i' 是单射，有 $a = -\alpha x_1$．用 $y_1 = -x_1$ 替换 x_1，从而正如所要的有 $(a, x_0) = (\alpha y_1, -jy_1) \in S$.

最后，定义 $\varphi: B \to B'$ 为

$$\varphi: (a, x_0) + S \mapsto f(a, x_0) = i'a + \beta' x_0$$

[因为 $B = (A \oplus X_0)/S$ 和 $S = \ker f$，所以 φ 是合理定义的]．为证明图

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{i} & B & \xrightarrow{\eta} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle 1_A} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle 1_C} & & \\ 0 & \longrightarrow & A & \xrightarrow{i'} & B' & \xrightarrow{\eta'} & C & \longrightarrow & 0 \end{array}$$

的交换性，我们用（i）中映射 i 和η的定义．关于第一个方块，如果 $a \in A$，则 $\varphi i a = \varphi((a,0) + S) = i'a$．关于第二个方块，

$$\begin{aligned} \eta'\varphi: (a, x_0) + S \mapsto \eta'(i'a + \beta' x_0) & \\ &= \eta' \beta' x_0 \\ &= \varepsilon x_0 \\ &= \eta((a, x_0) + S). \end{aligned}$$

所以，底下的两个行是等价扩张．■　858

记号　记刚构造的 A 和 C 的扩张为

$$\alpha \Xi.$$

对偶结果为真；它与用第二个变量 A 的内射分解构造的 Ext 相关．

引理 10.88　设 A 和 Y_0 都是模，并设 $\Xi': 0 \to A \to Y_0 \to Y_1 \to 0$ 是 A 与 Y_1 的扩张．给定模 C，考虑图

$$\begin{array}{ccccccccc} & & A & & & & C & & \\ & & \downarrow{\scriptstyle 1_A} & & & & \downarrow{\scriptstyle \gamma} & & \\ \Xi': 0 & \longrightarrow & A & \longrightarrow & Y_0 & \xrightarrow{p} & Y_1 & \longrightarrow & 0 \end{array}$$

（i）存在行正合的交换图完成给定的图：

$$\begin{array}{ccccccccc} \Xi'\gamma: 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle 1_A} & & \downarrow & & \downarrow{\scriptstyle \gamma} & & \\ \Xi': 0 & \longrightarrow & A & \longrightarrow & Y_0 & \xrightarrow{p} & Y_1 & \longrightarrow & 0 \end{array}$$

（ii）任意两个完成的图的顶上两行是等价扩张．

证明　这是引理 10.87 的对偶；特别地，用 γ 与 p 的拉回构造顶上一行．■

记号　记刚构造的 A 和 C 的扩张为

$$\Xi'\gamma.$$

定理 10.89　函数 $\psi: e(C, A) \to \operatorname{Ext}^1(C, A)$ 是双射．

证明　我们对ψ构造逆 $\theta: \operatorname{Ext}^1(C, A) \to e(C, A)$．选取 C 的一个投射分解，从而存在正合列

$$\cdots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \to C \to 0,$$

选取一个 1 -余圈 $\alpha: P_1 \to A$. 因 α 是余圈，有 $0 = d_2^*(\alpha) = \alpha d_2$，从而 α 诱导出同态 $\alpha': P_1/\mathrm{im}d_2 \to A$[如果 $x_1 \in P_1$，则 $\alpha': x_1 + \mathrm{im}\, d_2 \mapsto \alpha(x_1)$]. 令 Ξ 表示扩张

859

$$\Xi: 0 \to P_1/\mathrm{im}\, d_2 \to P_0 \to C \to 0.$$

和引理中一样，存在行正合的交换图：

$$\begin{array}{ccccccccc} 0 & \to & P_1/\mathrm{im}d_2 & \to & P_0 & \to & C & \to & 0 \\ & & \downarrow{\scriptstyle \alpha'} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle 1_C} & & \\ 0 & \to & A & \xrightarrow{i} & B & \to & C & \to & 0 \end{array}$$

用引理中的构造定义 $\theta: \mathrm{Ext}^1(C,A) \to e(C,A)$：

$$\theta(\alpha + \mathrm{im}d_1^*) = [\alpha'\Xi].$$

我们先证明 θ 不依赖于余圈 α 的选取. 假设 ζ 是陪集 $\alpha + \mathrm{im}d_1^*$ 的另一个代表元，则存在映射 $s: P_0 \to A$ 使得 $\zeta = \alpha + sd_1$. 但易知下面的图交换：

$$\begin{array}{ccccccccc} P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} & P_0 & \to & C & \to & 0 \\ \downarrow & & \downarrow{\scriptstyle \alpha+sd_1} & & \downarrow{\scriptstyle \beta+is} & & \downarrow{\scriptstyle 1_C} & & \\ 0 & \to & A & \xrightarrow{i} & B & \to & C & \to & 0 \end{array}$$

由于底下一行没有变，所以有 $[\alpha'\Xi] = [\zeta'\Xi]$.

剩下要证明复合 $\psi\theta$ 和 $\theta\psi$ 是恒等映射. 如果 $\alpha + \mathrm{im}d_1^* \in \mathrm{Ext}^1(C,A)$，则 $\theta(\alpha + \mathrm{im}d_1^*)$ 是图

$$\begin{array}{ccccccccc} 0 & \to & P_1/\mathrm{im}d_2 & \to & P_0 & \to & C & \to & 0 \\ & & \downarrow{\scriptstyle \alpha'} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle 1_C} & & \\ 0 & \to & A & \xrightarrow{i} & B & \to & C & \to & 0 \end{array}$$

的底下一行，且 $\psi\theta(\alpha + \mathrm{im}d_1^*)$ 是适合该图的一个余圈的同调类. 显然，α 就是这样的一个余圈；因此 $\psi\theta$ 是恒等映射. 关于另一个复合，从一个扩张 ξ 开始，然后把它嵌入图

$$\begin{array}{ccccccccc} P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} & P_0 & \to & C & \to & 0 \\ \downarrow & & \downarrow{\scriptstyle \alpha} & & \downarrow & & \downarrow{\scriptstyle 1_C} & & \\ 0 & \to & A & \xrightarrow{i} & B & \to & C & \to & 0 \end{array}$$

的底下一行. ξ 和 $\alpha'\Xi$ 都是这种图的底下一行，从而引理 10.87（ⅱ）证明 $[\xi] = [\alpha'\Xi]$. ■

860

我们现在证明命题 10.85 的逆.

系 10.90 对两个模 C 和 A，A 和 C 的每个扩张都是分裂的当且仅当 $\mathrm{Ext}_R^1(C,A) = \{0\}$.

证明 如果每个扩张都分裂，则 $|e(C,A)| = 1$，从而根据定理 10.89，$|\mathrm{Ext}_R^1(C,A)| = 1$；因此 $\mathrm{Ext}_R^1(C,A) = \{0\}$. 反之，如果 $\mathrm{Ext}_R^1(C,A) = \{0\}$，则命题 10.85 表明每个扩张都分裂. ■

例 10.91 如果 p 是素数，则在例 10.84（ⅰ）中我们看到 $\mathrm{Ext}_{\mathbb{Z}}^1(\mathbb{I}_p, \mathbb{I}_p) \cong \mathbb{I}_p$. 另一方面，由定理 10.89 可知扩张 $0 \to \mathbb{I}_p \to B \to \mathbb{I}_p \to 0$ 的等价类有 p 个. 但 $|B| = p^2$，因此如不计同构 B 只有两个选择：$B \cong \mathbb{I}_{p^2}$ 或 $B \cong \mathbb{I}_p \oplus \mathbb{I}_p$. 当然，这和例 10.18 是一致的. ■

下面是 Ext 的一个较次要的应用.

命题 10.92 (ⅰ) 如果 F 是无挠阿贝尔群而 T 是**阶有界**的阿贝尔群（即有某个正整数 n 使得 $nT = \{0\}$），则 $\mathrm{Ext}^1(F,T) = \{0\}$.

(ⅱ) 设 G 是阿贝尔群. 如果 G 的挠子群 tG 是阶有界的，则 tG 是 G 的直和项.

证明（i）因 F 是无挠的，根据系 9.6，它是一个平坦 $\mathbb{Z}$-模，因此 $0\to\mathbb{Z}\to\mathbb{Q}$ 的正合性给出 $0\to\mathbb{Z}\otimes F\to\mathbb{Q}\otimes F$ 的正合性．于是，$F\cong\mathbb{Z}\otimes F$ 可以嵌入 $\mathbb{Q}$ 上的一个向量空间 V，就是 $V=\mathbb{Q}\otimes F$. 运用反变函子 $\mathrm{Hom}(\ ,T)$ 到 $0\to F\to V\to V/F\to 0$ 得正合列

$$\mathrm{Ext}^1(V,T)\to\mathrm{Ext}^1(F,T)\to\mathrm{Ext}^2(V/F,T).$$

现在根据习题 10.39，最后一项是 $\{0\}$，和根据例 10.70，$\mathrm{Ext}^1(V,T)$ 是（无挠）可除的，从而 $\mathrm{Ext}^1(F,T)$ 是可除的．因 T 的阶有界，习题 10.41 给出 $\mathrm{Ext}^1(F,T)=\{0\}$.

（ii）要证明扩张 $0\to tG\to G\to G/tG\to 0$ 分裂，只需证明 $\mathrm{Ext}^1(G/tG,tG)=\{0\}$．因 G/tG 是无挠的，由（i）和系 10.90 可得结果． ■

一个群的挠子群可以不是直和项；下面用同调的证明和习题9.1(iii)的证明有很大的差别．

命题 10.93 *存在阿贝尔群 G，它的一个挠子群不是 G 的直和项；事实上，我们可以选取 $tG=\sum_p\mathbb{I}_p$，其中对一切素数 p 取和．*

861

证明　只需证明 $\mathrm{Ext}^1\left(\mathbb{Q},\sum_p\mathbb{I}_p\right)\neq 0$，这是因为它可给出不分裂扩张 $0\to\sum_p\mathbb{I}_p\to G\to\mathbb{Q}\to 0$；此外，因 $\mathbb{Q}$ 是无挠的，从而 $\sum_p\mathbb{I}_p=tG$.

考虑正合列 $0\to\sum_p\mathbb{I}_p\to\prod_p\mathbb{I}_p\to D\to 0$．根据习题 9.6，我们知道 D 是可除的（其实，$D\cong\mathbb{R}$；它是无挠可除群，因此根据命题 9.23，它是 $\mathbb{Q}$ 上的向量空间，我们可以验证 $\dim(D)=$ 连续统，它是 $\mathbb{R}$ 作为 $\mathbb{Q}$ 上的向量空间的维数）．存在正合列

$$\mathrm{Hom}\left(\mathbb{Q},\prod_p\mathbb{I}_p\right)\to\mathrm{Hom}(\mathbb{Q},D)\xrightarrow{\partial}\mathrm{Ext}^1\left(\mathbb{Q},\sum_p\mathbb{I}_p\right)\to\mathrm{Ext}^1\left(\mathbb{Q},\prod\mathbb{I}_p\right).$$

根据命题 10.81 和命题 10.92，∂ 是同构：$\mathrm{Ext}^1\left(\mathbb{Q},\prod_p\mathbb{I}_p\right)\cong\prod\mathrm{Ext}^1(\mathbb{Q},\mathbb{I}_p)=\{0\}$，又根据定理 7.33，$\mathrm{Hom}\left(\mathbb{Q},\prod_p\mathbb{I}_p\right)\cong\prod\mathrm{Hom}(\mathbb{Q},\mathbb{I}_p)=\{0\}$．因 $\mathrm{Hom}(\mathbb{Q},D)\neq\{0\}$，有 $\mathrm{Ext}^1\left(\mathbb{Q},\sum_p\mathbb{I}_p\right)\neq\{0\}$． ■

注　*我们可以证明一个挠阿贝尔群 T 有如下的性质：它是任一把它作为挠子群的群的直和项当且仅当 $T\cong B\oplus D$，其中 B 的阶有界且 D 是可除的．*

如果 $\mathcal{E}$ 是一个集合且 $\psi:\mathcal{E}\to G$ 是到群 G 的双射，则在 $\mathcal{E}$ 上存在唯一的群结构使它成为一个群且 ψ 是同构［如果 e, $e'\in\mathcal{E}$，则 $e=\psi^{-1}(g)$ 和 $e'=\psi^{-1}(g')$；定义 $ee'=\psi^{-1}(gg')$］．特别地，定理 10.89 蕴涵在 $e(C,A)$ 上存在群结构；下面是必要的定义．

定义**对角映射** $\Delta_C:C\to C\oplus C$ 为 $\Delta_C:c\mapsto(c,c)$，并定义**余对角映射** $\nabla_A:A\oplus A\to A$ 为 $\nabla_A:(a_1,a_2)\mapsto a_1+a_2$．注意，如果 $f,f':C\to A$ 是同态，则复合 $\nabla_A(f\oplus f')\Delta_C$ 是映射 $C\to C\oplus C\to A\oplus A\to A$. 容易验证 $\nabla_A(f\oplus f')\Delta_C=f+f'$，因此这个公式描述了 $\mathrm{Hom}(C,A)$ 中的加法．现在 Ext 是广义 Hom，因此我们模仿这个定义来定义 $e(C,A)$ 中的加法．

如果 $\xi:0\to A\to B\to C\to 0$ 和 $\xi':0\to A'\to B'\to C'\to 0$ 是扩张，则它们的直和是扩张

$$\xi\oplus\xi':0\to A\oplus A'\to B\oplus B'\to C\oplus C'\to 0.$$

白尔和 $[\xi]+[\xi']$ 是对等价类 $[\nabla_A(\xi\oplus\xi')\Delta_C]$ 定义的（我们已经定义了 $\alpha\Xi$ 和 $\Xi'\gamma$）．为证明白尔和是合理定义的，我们先证明 $\alpha(\Xi'\gamma)$ 和 $(\alpha\Xi')\gamma$ 等价．再证明 $\psi([\xi]+[\xi'])=\psi([\nabla_A(\xi\oplus\xi')\Delta_C])$，然后证明 $e(C,A)$ 在这个运算下是群．幺元是分裂扩张的类，$[\xi]$ 的逆是 $[(-1_A)\xi]$.

Ext^1 的这个描述已经由米田信夫加以推广，他对一切 n 描述了 Ext^n．米田信夫的 $\mathrm{Ext}^n(C,A)$

的元素是正合列

$$0 \to A \to B_1 \to \cdots \to B_n \to C \to 0$$

862 的某种等价类，且用一个广义白尔和把它们加起来（见 Mac Lane 所著的《Homology》，82～87页）．于是，存在 Ext 的不用导函子的构造法．事实上，我们可以不用投射和内射构造 Ext^n．

奥斯兰德（M. Auslander）和赖滕（I. Reiten）在研究有限维代数时引入如下的概念．

定义 *称环 R 上一个左 R-模的正合列*

$$\Xi: 0 \to N \to X \to M \to 0$$

*为**殆分裂**，如果它不分裂，如果 N 和 M 都是不可分解模，且对一切 R-模 C 和每个不是同构的 R-映射 $\varphi: C \to M$，正合列 $\Xi\varphi$ 分裂．*

换句话说，Ξ 是 $\mathrm{Ext}_R^1(N,M)$的非零元素，其中 N 和 M 都是不可分解的，且对每个不是同构的 $\varphi: C \to M, \Xi \in \ker\varphi^*$．奥斯兰德和赖滕证明对每个不是投射的不可分解模 M，存在以 M 结尾的殆分裂的正合列．对偶地，他们证明对每个不是内射的不可分解模 N，存在以 N 起首的殆分裂的正合列．

现在转而讨论 Tor. 我们先给出和 Ext 不类似的一个结果．

定理 10.94 *如果 R 是环，A 是右 R-模，B 是左 R-模，则对一切 $n \geqslant 0$，*

$$\mathrm{Tor}_n^R(A,B) \cong \mathrm{Tor}_n^{R^{op}}(B,A),$$

其中 R^{op} 是 R 的对立环．

证明 回忆命题 8.11：每个左 R-模是一个右 R^{op}-模，每个右 R-模是一个左 R^{op}-模．选取 A 的一个删除投射分解 $\mathbf{P}_A$．易知 $t: \mathbf{P}_A \otimes_R B \to B \otimes_{R^{op}} \mathbf{P}_A$ 是$\mathbb{Z}$-复形的链映射，其中

$$t_n: P_n \otimes_R B \to B \otimes_{R^{op}} P_n$$

由

$$t_n: x_n \otimes b \mapsto b \otimes x_n$$

给出．因每个 t_n 是阿贝尔群的同构（它的逆是 $b \otimes x_n \mapsto x_n \otimes b$），根据习题 10.22，对一切 n，链映射 t 是复形的同构，

$$\mathrm{Tor}_n^R(A,B) = H_n(\mathbf{P}_A \otimes_R B) \cong H_n(B \otimes_{R^{op}} \mathbf{P}_A).$$

但看作左 R^{op}-模的复形的 $\mathbf{P}_A$ 是 A 作为左 R^{op}-模的删除投射分解，因此 $H_n(B \otimes_{R^{op}} \mathbf{P}_A) \cong \mathrm{Tor}_n^{R^{op}}(B,A)$. ∎

根据这个结果，关于 $\mathrm{Tor}(A, \ )$的定理产生关于 $\mathrm{Tor}(\ ,B)$的结果；我们不必再说“对另一个变

863 量有类似的结果”．

系 10.95 *如果 R 是交换环且 A，B 是 R-模，则对一切 $n \geqslant 0$，*

$$\mathrm{Tor}_n^R(A,B) \cong \mathrm{Tor}_n^R(B,A).$$

我们知道 Tor_n 在投射模上消失；现在证明它在平坦模上消失．

命题 10.96 *右 R-模是平坦的当且仅当对一切 $n \geqslant 1$ 和每个左 R-模 M，$\mathrm{Tor}_n^R(F,M) = \{0\}$．*

证明 设 $0 \to N \xrightarrow{i} P \to M \to 0$ 是正合的，其中 P 是投射的．存在正合列

$$\mathrm{Tor}_1(F,P) \to \mathrm{Tor}_1(F,M) \to F \otimes N \xrightarrow{1 \otimes i} F \otimes P.$$

现在因为 P 是投射的，所以 $\mathrm{Tor}_1(F,P) = \{0\}$，从而 $\mathrm{Tor}_1(F,M) = \ker(1 \otimes i)$．然而，因 F 是平坦

的，$\ker(1\otimes i)=\{0\}$，因此 $\mathrm{Tor}_1(F,M)=\{0\}$. 该结果可对一切 $n\geqslant 1$ 用长度推移法得到.

关于逆命题，$0\to A\xrightarrow{i}B$ 正合蕴涵

$$0=\mathrm{Tor}_1(F,B/A)\to F\otimes A\xrightarrow{1\otimes i}F\otimes B$$

的正合性. 因此，$1\otimes i$ 是单射，从而 F 是平坦的.（注意在逆命题的证明中，我们只假设 Tor_1 消失.）■

命题 10.97 *如果 $\{B_k:k\in K\}$ 是左 R-模的族，则对一切 n 存在自然同构，*

$$\mathrm{Tor}_n^R\Big(A,\sum_{k\in K}B_k\Big)\cong\sum_{k\in K}\mathrm{Tor}_n^R(A,B_k).$$

如果在第一个变量中取和，也存在同构.

证明 用长度推移法证明. 基础步是定理 8.87，因为 $\mathrm{Tor}_0(A,\ )$ 和 $A\otimes$ 自然等价.

关于归纳步，对每个 $k\in K$，选取短正合列

$$0\to N_k\to P_k\to B_k\to 0,$$

其中 P_k 是投射的. 存在正合列

$$0\to\sum_k N_k\to\sum_k P_k\to\sum_k B_k\to 0,$$

因为投射模的和是投射的，所以 $\sum_k P_k$ 是投射的. 存在行正合的交换图

$$\begin{array}{ccccccc}
\mathrm{Tor}_1(A,\Sigma P_k) & \longrightarrow & \mathrm{Tor}_1(A,\Sigma B_k) & \xrightarrow{\partial} & A\otimes\Sigma N_k & \longrightarrow & A\otimes\Sigma P_k\\
 & & \downarrow & & \downarrow{\scriptstyle\tau} & & \downarrow{\scriptstyle\sigma}\\
\Sigma\,\mathrm{Tor}_1(A,P_k) & \longrightarrow & \Sigma\,\mathrm{Tor}_1(A,B_k) & \xrightarrow{\partial'} & \Sigma\, A\otimes N_k & \longrightarrow & \Sigma A\otimes P_k
\end{array}$$

864

其中底下一行的映射恰是每个坐标中的通常的诱导映射，映射 τ 和 σ 是定理 8.87 给出的同构. 证明由长度推移法完成. ■

例 10.98 （i）我们证明，对每个阿贝尔群 B，

$$\mathrm{Tor}_1^{\mathbb{Z}}(\mathbb{I}_n,B)\cong B[n]=\{b\in B:nb=0\}.$$

存在正合列

$$0\to\mathbb{Z}\xrightarrow{\mu_n}\mathbb{Z}\to\mathbb{I}_n\to 0,$$

其中 μ_n 是乘 n. 运用 $\otimes B$ 给出

$$\mathrm{Tor}_1(\mathbb{Z},B)\to\mathrm{Tor}_1(\mathbb{I}_n,B)\to\mathbb{Z}\otimes B\xrightarrow{1\otimes\mu_n}\mathbb{Z}\otimes B$$

的正合性. 现在因为$\mathbb{Z}$是投射的，所以 $\mathrm{Tor}_1(\mathbb{Z},B)=\{0\}$. 此外，$1\otimes\mu_n$ 也是乘 n，而$\mathbb{Z}\otimes B=B$. 更精确地说，$\mathbb{Z}\otimes$ 和 **Ab** 上的单位函子自然等价，因此存在行正合的交换图

$$\begin{array}{ccccccc}
0 & \longrightarrow & B[n] & \longrightarrow & B & \xrightarrow{\mu_n} & B\\
 & & \downarrow & & \downarrow{\scriptstyle\tau_B} & & \downarrow{\scriptstyle\tau_B}\\
0 & \longrightarrow & \mathrm{Tor}_1(\mathbb{I}_n,B) & \longrightarrow & \mathbb{Z}\otimes B & \xrightarrow{1\otimes\mu_n} & \mathbb{Z}\otimes B
\end{array}$$

根据命题 8.94，存在同构 $B[n]\cong\mathrm{Tor}_1(\mathbb{I}_n,B)$.

（ii）现在只要 A 和 B 都是有限生成阿贝尔群，我们就能够计算 $\mathrm{Tor}_1^{\mathbb{Z}}(A,B)$. 根据基本定理，$A$ 和 B 都是循环群的直和. 因 Tor 与直和交换，$\mathrm{Tor}_1^{\mathbb{Z}}(A,B)$是群 $\mathrm{Tor}_1^{\mathbb{Z}}(C,D)$的直和，其中 C 和 D 都是循环群. 可以假定 C 和 D 都是有限的，否则它们是投射的且 $\mathrm{Tor}_1=\{0\}$. 这个计算可用（i）和

习题 5.6 完成，它说如果 D 是有有限阶 m 的循环群，则 $D[n]$是 d 阶循环群，其中 $d=(m,n)$是它们的 gcd. ■

和 Ext 对照，命题 10.97 可以通过把和换成正向极限而加以推广.

命题 10.99 *如果 $\{B_i\varphi_j^i\}$ 是有向指标集 I 上左 R-模的正系统，则对一切右 R-模 A 和一切 $n\geqslant 0$，存在同构*

$$\mathrm{Tor}_n^R(A,\varinjlim B_i)\cong\varinjlim \mathrm{Tor}_n^R(A,B_i).$$

865

证明 用长度推移法证明．基础步是定理 8.101，因为 $\mathrm{Tor}_0(A,\ )$和 $A\otimes$ 自然等价．

关于归纳步，对每个 $i\in I$ 选取一个短正合列

$$0\to N_i\to P_i\to B_i\to 0,$$

其中 P_i 是投射的．因指标集是有向的，命题 7.100 说存在正合列

$$0\to\varinjlim N_i\to\varinjlim P_i\to\varinjlim B_i\to 0.$$

现在因为每个投射模是平坦的，并根据系 8.102，平坦模的正向极限也是平坦的，所以$\varinjlim P_i$ 是平坦的．存在行正合的交换图：

$$\begin{array}{ccccccc}
\mathrm{Tor}_1(A,\varinjlim P_i) & \to & \mathrm{Tor}_1(A,\varinjlim B_i) & \xrightarrow{\partial} & A\otimes\varinjlim N_i & \to & A\otimes\varinjlim P_i\\
 & & \downarrow & & \downarrow\tau & & \downarrow\sigma\\
\varinjlim\mathrm{Tor}_1(A,P_i) & \to & \varinjlim\mathrm{Tor}_1(A,B_i) & \xrightarrow{\vec{\partial}} & \varinjlim A\otimes N_i & \to & \varinjlim A\otimes P_i
\end{array}$$

其中底下一行的映射恰是正向极限之间的通常的诱导映射，且映射 τ，σ 都是定理 8.101 给出的同构．对 $n\geqslant 2$ 的证明是很容易的． ■

上面的命题推广了引理 8.97，它说如果模 M 的每个有限生成子模是平坦的，则 M 自身也是平坦的．毕竟，根据例7.97(iv)，M 是它的有限生成子模在一个有向指标集上的正向极限．

当环 R 非交换时，$A\otimes_R B$ 是阿贝尔群，但它未必是 R-模．

命题 10.100 （i）*设 $r\in Z(R)$是一个中心元素，设 A 是右 R-模，并设 B 是左 R-模．如果 $\mu_r:B\to B$ 是乘 r，则诱导映射*

$$\mu_{r*}:\mathrm{Tor}_n^R(A,B)\to\mathrm{Tor}_n^R(A,B)$$

也是乘 r.

（ii）*如果 R 是交换环，则 $\mathrm{Tor}_n^R(A,B)$是 R-模．*

证明 （i）从例 10.47 立即可得．

（ii）如果定义乘标量 r 为 μ_{r*}，则从（i）可得结果． ■

866

现在假定 R 是整环，从而挠子模的概念有定义，我们将看到 Tor 这个名称的由来．

引理 10.101 *设 R 是整环，$Q=\mathrm{Frac}(R)$，并设 $K=Q/R$.*

（i）*如果 A 是挠 R-模，则 $\mathrm{Tor}_1^R(K,A)\cong A$.*

（ii）*对每个 R-模 A，对一切 $n\geqslant 2$，$\mathrm{Tor}_n(K,A)=\{0\}$.*

（iii）*如果 A 是无挠 R-模，则 $\mathrm{Tor}_1(K,A)=\{0\}$.*

证明 （i）$0\to R\to Q\to K\to 0$ 的正合性给出

$$\mathrm{Tor}_1(Q,A)\to\mathrm{Tor}_1(K,A)\to R\otimes A\to Q\otimes A$$

的正合性．现在根据系 8.103，Q是平坦的，因此根据命题 10.96，$\mathrm{Tor}_1(Q,A)=\{0\}$．因为$Q$是可除的和 A 是挠的，根据习题 9.15，最后一项 $Q\otimes A=\{0\}$，从而中间映射 $\mathrm{Tor}_1(K,A)\to R\otimes A$ 是同构．

（ii）存在正合列

$$\mathrm{Tor}_n(Q,A) \to \mathrm{Tor}_n(K,A) \to \mathrm{Tor}_{n-1}(R,A).$$

因 $n\geqslant 2$，有 $n-1\geqslant 1$，由于 Q 和 R 都是平坦的，因此第一个和第三个 Tor 是 $\{0\}$. 所以，正合性给出 $\mathrm{Tor}_n(K,A)=\{0\}$.

（ⅲ）根据定理 8.104，存在内射 R-模 E 包含 A 并把它作为子模. 然而，因 A 是无挠的，$A\cap tE=\{0\}$，从而 A 嵌入 E/tE. 根据引理 7.72，内射模是可除的，所以 E 是可除的，因而商 E/tE 是可除的. 现在因为 E/tE 是无挠可除 R-模，所以 E/tE 是 Q 上的向量空间（习题 9.7）. 记 E/tE 为 V. 因每个向量空间有基，所以 V 是 Q 的复制的直和. 系 8.103 说 Q 是平坦的，引理 8.98 说平坦模的直和是平坦的. 由此可知 V 是平坦的[⊖].

$0\to A\to V\to V/A\to 0$ 的正合性给出

$$\mathrm{Tor}_2(K,V/A)\to\mathrm{Tor}_1(K,A)\to\mathrm{Tor}_1(K,V)$$

的正合性. 现在根据（ⅱ），$\mathrm{Tor}_2(K,V/A)=\{0\}$，因 V 是平坦的，所以 $\mathrm{Tor}_1(K,V)=\{0\}$. 从正合性可知 $\mathrm{Tor}_1(K,A)=\{0\}$. ■

下一结果表明 Tor 这个名称的由来.

定理 10.102 （ⅰ）如果 R 是整环，$Q=\mathrm{Frac}(R)$，$K=Q/R$，则函子 $\mathrm{Tor}_1^R(K,\ )$ 和挠函子自然等价.

（ⅱ）对一切 R-模 A，$\mathrm{Tor}_1^R(K,A)\cong tA$.

证明

$$\mathrm{Tor}_2(K,A/tA)\to\mathrm{Tor}_1(K,tA)\xrightarrow{\iota_A}\mathrm{Tor}_1(K,A)\to\mathrm{Tor}_1(K,A/tA)$$

的正合性，根据引理10.101(ⅱ)，第一项是 $\{0\}$，根据引理10.101(ⅲ)，最后一项是 $\{0\}$. 所以，映射 $\iota_A:\mathrm{Tor}_1(K,tA)\to\mathrm{Tor}_1(K,A)$ 是同构.

设 $f:A\to B$，并设 $f':tA\to tB$ 是它的限制. 因为 $\mathrm{Tor}_1(K,\ )$ 是函子，所以下面的图交换，这就是说，同构 ι_A 组成自然变换.

$$\begin{array}{ccc}\mathrm{Tor}_1(K,tA) & \xrightarrow{\iota_A} & \mathrm{Tor}_1(K,A)\\ \downarrow f'_* & & \downarrow f_*\\ \mathrm{Tor}_1(K,tB) & \xrightarrow{\iota_B} & \mathrm{Tor}_1(K,B)\end{array}$$

■

存在由生成元和关系组成的 $\mathrm{Tor}_1^{\mathbb{Z}}(A,B)$ 的构造. 考虑一切三元组 (a,n,b)，其中 $a\in A$，$b\in B$，$na=0$ 和 $nb=0$. 则 $\mathrm{Tor}_1^{\mathbb{Z}}(A,B)$ 由一切这样的三元组在关系

$$(a+a',n,b)=(a,n,b)+(a',n,b)$$
$$(a,n,b+b')=(a,n,b)+(a,n,b')$$
$$(ma,n,b)=(a,mn,b)=(a,m,nb)$$

（只要两边都有定义）的制约下生成. 关于这个结果的证明以及对任意环 R 到 $\mathrm{Tor}_n^R(A,B)$ 的推广，见 Mac Lane 所著的《Homology》，150～159 页.

Tor 函子在代数拓扑中是非常有用的. 万有系数定理对系数在一个阿贝尔群 G 中的同调群 $H_n(X;G)$ 给出一个公式.

定理（万有系数） 关于每个拓扑空间 X 和每个阿贝尔群 G，对一切 $n\geqslant 0$ 存在同构

⊖ 无挠 $\mathbb{Z}$-模是平坦的，但存在这样的整环 R，它有不平坦的无挠模. 事实上，每个无挠模都是平坦的整环叫做普吕弗环，它被刻画为这样的整环，其中每个有限生成理想都是投射模.

$$H_n(X;G) \cong H_n(X) \otimes_{\mathbf{Z}} G \oplus \mathrm{Tor}_1^{\mathbf{Z}}(H_{n-1}(X),G).$$

证明 见 Rotman 所著的《An Introduction to Algebraic Topology》，261 页． ■

如果知道空间 X 和 Y 的同调群，则屈内特公式对 $X \times Y$ 的同调群给出一个公式，这在本质上也涉及 Tor.

定理（屈内特公式） 关于每对拓扑空间 X 和 Y，对每个 $n \geq 0$ 存在同构，

$$H_n(X \times Y) \cong \sum_i H_i(X) \otimes_{\mathbf{Z}} H_{n-i}(Y) \oplus \sum_p \mathrm{Tor}_1^{\mathbf{Z}}(H_p(X),H_{n-1-p}(Y)).$$

证明 见 Rotman 所著的《An Introduction to Algebraic Topology》，269 页． ■

习题

10.44 证明类似定理 10.45 的如下命题．设 $\mathcal{E}^n : {}_R\mathbf{Mod} \to \mathbf{Ab}$ 是共变函子的序列，对 $n \geq 0$，满足

（i）对每个短正合列 $0 \to A \to B \to C \to 0$，存在长正合列和自然连接同态

$$\cdots \to \mathcal{E}^n(A) \to \mathcal{E}^n(B) \to \mathcal{E}^n(C) \xrightarrow{\Delta_n} \mathcal{E}^{n+1}(A) \to \cdots;$$

（ii）存在左 R-模 M 使得 $\mathcal{E}^0$ 和 $\mathrm{Hom}_R(M,\ )$ 自然等价．

（iii）对一切内射模 E 和一切 $n \geq 1$，$\mathcal{E}^n(E) = \{0\}$.

证明对一切 $n \geq 0$，$\mathcal{E}^n$ 和 $\mathrm{Ext}^n(M,\ )$ 自然等价．

10.45 设 $\mathrm{TOR}^n : {}_R\mathbf{Mod} \to \mathbf{Ab}$ 是共变函子的序列，对 $n \geq 0$，满足

（i）对每个短正合列 $0 \to A \to B \to C \to 0$，存在长正合列和自然连接同态

$$\cdots \to \mathrm{TOR}_n(A) \to \mathrm{TOR}_n(B) \to \mathrm{TOR}_n(C) \xrightarrow{\Delta_n} \mathrm{TOR}_{n-1}(A) \to \cdots;$$

（ii）存在左 R-模 M 使得 TOR_0 和 $\otimes_R M$ 自然等价．

（iii）对一切投射模 P 和一切 $n \geq 1, \mathrm{TOR}_n(P) = \{0\}$.

证明对一切 $n \geq 0, \mathrm{TOR}_n$ 和 $\mathrm{Tor}_n(\ ,M)$ 自然等价．（如果固定第一个变量，则有类似的结果．）

10.46 证明模 A 和 C 的任意两个分裂扩张等价．

10.47 证明：如果 A 是阿贝尔群，且有某个正整数 n 使得 $nA = A$，则每个扩张 $0 \to A \to E \to \mathbf{I}_n \to 0$ 分裂．

10.48 如果 A 是挠阿贝尔群，证明 $\mathrm{Ext}^1(A,\mathbf{Z}) \cong \mathrm{Hom}(A,S^1)$，其中 S^1 是圆群．

10.49 证明左 R-模 E 是内射模当且仅当对每个左 R-模 $A, \mathrm{Ext}_R^1(A,E) = \{0\}$.

10.50 对任意环 R，证明左 R-模 B 是内射模当且仅当对每个左理想 I，$\mathrm{Ext}^1(R/I,B) = \{0\}$.

提示：用白尔判别法．

10.51 证明阿贝尔群 G 是内射的当且仅当 $\mathrm{Ext}^1(\mathbf{Q}/\mathbf{Z},G) = \{0\}$.

10.52 证明阿贝尔群 G 是自由阿贝尔群当且仅当对每个自由阿贝尔群 $F, \mathrm{Ext}^1(G,F) = \{0\}$.[⊖]

10.53 如果 $0 \to A \to B \to C \to 0$ 是右 R-模的正合列，且 A 和 C 都是平坦的，证明 B 也是平坦的．

10.54 如果 A 和 B 都是有限阿贝尔群，证明 $\mathrm{Tor}_1^{\mathbf{Z}}(A,B) \cong A \otimes_{\mathbf{Z}} B$.

10.55 设 R 是整环，$Q = \mathrm{Frac}(R), K = Q/R$.

（i）证明：对每个 R-模 A，存在正合列

$$0 \to tA \to A \to Q \otimes A \to K \otimes A \to 0.$$

（ii）证明模 A 是挠的当且仅当 $Q \otimes A = \{0\}$.

10.56 设 R 是整环．

⊖ $\mathrm{Ext}^1(G,\mathbf{Z}) = \{0\}$ 是否蕴涵 G 是自由阿贝尔群的问题作为怀特黑德问题而知名．由此引出这样的结果：如果 G 是可数的，则它必是自由阿贝尔群，但谢拉赫（S. Shelah）证明这样的不可数 G 是否必是自由阿贝尔群是不可判定的．

（ⅰ）如果 B 是挠 R-模，证明对一切 R-模 A 和一切 $n\geqslant 0$，$\mathrm{Tor}_n(A,B)$ 是挠 R-模．

（ⅱ）对一切 R-模 A 和 B，证明对一切 $n\geqslant 1$，$\mathrm{Tor}_n(A,B)$ 是挠 R-模．

10.57　设 k 是域，设 $R=k[x,y]$，并设 I 是理想 (x,y)．

（ⅰ）证明 $x\otimes y-y\otimes x\in I\otimes_R I$ 是非零元素．

提示：考虑 $(I/I^2)\otimes(I/I^2)$．

（ⅱ）证明 $x(x\otimes y-y\otimes x)=0$，并由此推出 $I\otimes_R I$ 不是无挠的．

10.7　群的上同调

回忆命题 10.30 和命题 10.31 说存在正合列

$$F_3\xrightarrow{d_3}F_2\xrightarrow{d_2}F_1\xrightarrow{d_1}F_0\to\mathbb{Z}\to 0,$$

其中 F_0，F_1，F_2 和 F_3 都是自由 Q-模且 $\mathbb{Z}$ 看作平凡 Q-模．根据 10.3 节的计算，下面的定义现在看起来是合理的．

定义　*设 G 是群，设 A 是 G-模（即左 $\mathbb{Z}G$-模），并设 $\mathbb{Z}$ 是看作平凡 G-模的整数（即对一切 $g\in G$ 和 $m\in\mathbb{Z}$，$gm=m$）．G 的***上同调群***是*

$$H^n(G,A)=\mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z},A);$$

*G 的***同调群***是*

$$H_n(G,A)=\mathrm{Tor}^{\mathbb{Z}G}_n(\mathbb{Z},A).$$

群的上同调的历史是十分有趣的．这个课题起源于 20 世纪 30 年代拓扑学家胡尔维茨（W. Hurewicz）的发现，即如果 X 是一个连通非球面空间（用现代语言来说，如果 X 的高次同调群都是平凡的），则 X 的一切同调和上同调群都由基本群 $\pi=\pi_1(X)$ 确定．由此引出 $H_n(X)$ 是否能用 π 代数地描述的问题．例如，胡尔维茨证明 $H_1(X)\cong\pi/\pi'$，其中 π' 是换位子群．1942 年，霍普夫（H. Hopf）证明，如果 π 有表现 F/R，其中 F 是自由的，则 $H_2(X)\cong(R\cap F')/[F,R]$，其中 $[F,R]$ 是由一切形如 $frf^{-1}r^{-1}$（其中 $f\in F$，$r\in R$）的换位子生成的子群．这些结果导致艾伦伯格、麦克莱恩、霍普夫、弗赖登塔尔和埃克曼创造了群的上同调．

接下来，我们用记 $\mathrm{Hom}_{\mathbb{Z}G}$ 为 Hom_G，记 $\otimes_{\mathbb{Z}G}$ 为 $\otimes_G$．因为平凡 G-模 $\mathbb{Z}$ 的特殊作用，由

$$\varepsilon:\sum_{x\in G}m_x x\mapsto\sum_{x\in G}m_x$$

定义的增广映射

$$\varepsilon:\mathbb{Z}G\to\mathbb{Z}$$

是重要的．回忆在习题 8.37 中我们已经看到 ε 是环满同态，因此它的核 $\mathcal{G}$ 是 $\mathbb{Z}G$ 中的双边理想，称为**增广理想**．于是，存在正合列

$$0\to\mathcal{G}\to\mathbb{Z}G\xrightarrow{\varepsilon}\mathbb{Z}\to 0.$$

命题 10.103　*设 G 是有增广理想 $\mathcal{G}$ 的群．作为阿贝尔群，$\mathcal{G}$ 是以 $G-1=\{x-1:x\in G,x\neq 1\}$ 为基的自由阿贝尔群．*

证明　元素 $u=\sum_x m_x x\in\mathbb{Z}G$ 在 $\ker\varepsilon=\mathcal{G}$ 中当且仅当 $\sum_x m_x=0$．所以，如果 $u\in\mathcal{G}$，则

$$u=u-\Big(\sum_x m_x\Big)1=\sum_x m_x(x-1).$$

于是，对 $x\in G$，$\mathcal{G}$ 由非零元素 $x-1$ 生成．

假设 $\sum_{x\neq 1} n_x(x-1)=0$，则在$\mathbb{Z}G$中 $\sum_{x\neq 1} n_x x-\left(\sum_{x\neq 1} n_x\right)1=0$，$\mathbb{Z}G$作为阿贝尔群是以$G$的元素为基的自由阿贝尔群．因此，对一切 $x\neq 1$，$n_x=0$．所以，非零 $x-1$ 组成$\mathcal{G}$的基． ■

我们先考察同调群．

命题 10.104 如果 A 是 G-模，则

$$H_0(G,A)=\mathbb{Z}\otimes_G A\cong A/\mathcal{G}A.$$

证明 根据定义，$H_0(G,A)=\mathrm{Tor}_0^{\mathbb{Z}G}(\mathbb{Z},A)=\mathbb{Z}\otimes_G A$. 运用右正合函子 $\otimes_G A$ 到正合列

$$0\to\mathcal{G}\to\mathbb{Z}G\to\mathbb{Z}\to 0$$

得下面交换图的第一行的正合性：

$$\begin{array}{ccccccc}\mathcal{G}\otimes_G A & \longrightarrow & \mathbb{Z}G\otimes_G A & \longrightarrow & \mathbb{Z}\otimes_G A & \longrightarrow & 0\\ \downarrow & & \downarrow & & \vdots & & \\ \mathcal{G}A & \longrightarrow & A & \longrightarrow & A/\mathcal{G}A & \longrightarrow & 0\end{array}$$

两个垂直实箭头由 $u\otimes a\mapsto ua$ 给出．根据命题 8.93，存在同构 $\mathbb{Z}\otimes_G A\cong A/\mathcal{G}A$. ■

易知 $A/\mathcal{G}A$ 是 G-平凡的；事实上，它是 A 的最大 G-平凡商．

例 10.105 假设 E 是阿贝尔群 A 和群 G 的半直积．回忆$[G,A]$是由一切形如$[x,a]=xax^{-1}a^{-1}$（其中 $x\in G$和$a\in A$）的换位子生成的子群．如果像本章开始的那样把换位子群写作加性的，则

$$[x,a]=x+a-x-a=xa-a=(x-1)a$$

（回忆 G 由共轭作用在 A 上）．所以这里 $A/\mathcal{G}A=A/[G,A]$. ■

我们现在用投射分解选取的无关性计算有限循环群 G 的同调群．

引理 10.106 设 $G=\langle x\rangle$ 是有有限阶 k 的循环群．定义$\mathbb{Z}G$中的元素 D 和 N 为

$$D=x-1 \text{ 和 } N=1+x+x^2+\cdots+x^{k-1}.$$

则下列序列是$\mathbb{Z}$的 G-自由分解：

$$\cdots\to\mathbb{Z}G\xrightarrow{N}\mathbb{Z}G\xrightarrow{D}\mathbb{Z}G\xrightarrow{N}\mathbb{Z}G\xrightarrow{D}\mathbb{Z}G\xrightarrow{\varepsilon}\mathbb{Z}\to 0,$$

其中 ε 是增广映射，而其他映射分别是乘 N 和乘 D.

证明 显然，每个项$\mathbb{Z}G$是自由的，而且，因$\mathbb{Z}G$是交换的，映射都是 G-映射．现在 $DN=ND=x^k-1=0$，而如果 $u\in\mathbb{Z}G$，则因为 ε 是环映射，有

$$\varepsilon D(u)=\varepsilon((x-1)u)=\varepsilon(x-1)\varepsilon(u)=0,$$

于是有一个复形，且剩下的只需证明正合性．

我们已经注意到 ε 是满射．现在根据命题 10.103，$\ker\varepsilon=\mathcal{G}=\mathrm{im}D$，因此在第零步有正合性．

假设 $u=\sum_{i=0}^{k-1} m_i x^i\in\ker D$；即 $(x-1)u=0$．展开并用$\mathbb{Z}G$以 $\{1,x,x^2,\cdots,x^{k-1}\}$ 为基的事实，有

$$m_0=m_1=\cdots=m_{k-1},$$

因此正如所要的 $u=m_0N\in\mathrm{im}N$.

最后，如果 $u=\sum_{i=0}^{k-1} m_i x^i\in\ker N$，则 $0=\varepsilon(Nu)=\varepsilon(N)\varepsilon(u)=k\varepsilon(u)$，因此 $\varepsilon(u)=\sum_{i=0}^{k-1} m_i=0$. 所以

$$u=-D\left(m_0 1+(m_0+m_1)x+\cdots+(m_0+\cdots+m_{k-1})x^{k-1}\right)\in\mathrm{im}D.$$ ■

定义 如果 A 是 G-模,定义子模

$$A[N]=\{a\in A: Na=0\}$$

和

$$A^G=\{a\in A:对一切\ g\in G, ga=a\}.$$

定理 10.107 如果 G 是有有限阶 k 的循环群且 A 是 G-模,则

$$H_0(G,A)=A/\mathcal{G}A;$$

$$对一切\ n\geqslant 1, H_{2n-1}(G,A)=A^G/NA;$$

$$对一切\ n\geqslant 1, H_{2n}(G,A)=A[N]/\mathcal{G}A.$$

证明 运用 $\otimes_G A$ 到引理 10.106 中Z的分解上,注意Z$G\otimes_G A\cong A$. 现在容易计算 ker/im, 用 $D=\mathcal{G}A$, 它来自命题 10.103 和 $(x-1)|(x^i-1)$ 的事实. ■

系 10.108 如果 G 是 k 阶有限循环群且 A 是平凡 G-模, 则

$$H_0(G,A)=A;$$

$$对一切\ n\geqslant 1, H_{2n-1}(G,A)=A/kA;$$

$$对一切\ n\geqslant 1, H_{2n}(G,A)=A[k].$$

特别地,

$$H_0(G,\mathbb{Z})=\mathbb{Z};$$

$$对一切\ n\geqslant 1, H_{2n-1}(G,\mathbb{Z})=\mathbb{Z}/k\mathbb{Z};$$

$$对一切\ n\geqslant 1, H_{2n}(G,\mathbb{Z})=\{0\}.$$

证明 因 A 是 G-平凡的, 有 $A^G=A$ 和 $\mathcal{G}A=\{0\}$ {因为 $xa=a$, 从而 $Da=(x-1)a=0$}. ■

我们现在计算未必是循环群的低维同调群.

引理 10.109 对任意群 G, 有

$$H_1(G,\mathbb{Z})\cong \mathcal{G}/\mathcal{G}^2.$$

证明 由

$$0\to\mathcal{G}\to\mathbb{Z}G\xrightarrow{\varepsilon}\mathbb{Z}\to 0$$

产生的长正合列以

$$H_1(G,\mathbb{Z}G)\to H_1(G,\mathbb{Z})\xrightarrow{\partial} H_0(G,\mathcal{G})\to H_0(G,\mathbb{Z}G)\xrightarrow{\varepsilon_*} H_0(G,\mathbb{Z})\to 0$$

结尾. 现在 $H_1(G,\mathbb{Z}G)=\{0\}$, 这是因为ZG 是投射的, 从而 ∂ 是单射. 又根据命题 10.104,

$$H_0(G,\mathbb{Z}G)\cong\mathbb{Z}.$$

因 ε_* 是满射, 它也必是单射(如果 $\ker\varepsilon_*\neq\{0\}$, 则 $\mathbb{Z}/\ker\varepsilon_*$ 是有限的; 另一方面, $\mathbb{Z}/\ker\varepsilon_*\cong\mathrm{im}\,\varepsilon_*=\mathbb{Z}$, 它是无挠的). 现在同调群序列的正合性($\partial$ 是满射当且仅当 ε_* 是单射)给出满射∂. 由此根据命题 10.104, ■

$$\partial: H_1(G,\mathbb{Z})\cong H_0(G,\mathcal{G})\cong\mathcal{G}/\mathcal{G}^2.$$

命题 10.110 对于任意群 G, 有

$$H_1(G,\mathbb{Z})\cong G/G',$$

其中 G' 是 G 的换位子群.

证明 只需证明 $G/G'\cong\mathcal{G}/\mathcal{G}^2$. 定义 $\theta: G\to\mathcal{G}/\mathcal{G}^2$ 为

$$\theta: x \mapsto (x-1)+\mathcal{G}^2.$$

为证明 θ 是同态，注意

$$xy-1-(x-1)-(y-1)=(x-1)(y-1)\in\mathcal{G}^2,$$

因此

$$\begin{aligned}\theta(xy) &= xy-1+\mathcal{G}^2\\ &= (x-1)+(y-1)+\mathcal{G}^2\\ &= x-1+\mathcal{G}^2+y-1+\mathcal{G}^2\\ &= \theta(x)+\theta(y).\end{aligned}$$

因 $\mathcal{G}/\mathcal{G}^2$ 是阿贝尔群，$G'\subseteq\ker\theta$，因此 θ 诱导同态 $\theta': G/G'\to\mathcal{G}/\mathcal{G}^2$，就是 $xG'\mapsto x-1+\mathcal{G}^2$.

我们现在构造 θ' 的逆．根据命题 10.103，$\mathcal{G}$ 是以一切 $x-1$ 为基的自由阿贝尔群，其中 $x\in G$ 且 $x\neq 1$ 由此存在（合理定义的）同态 $\varphi: \mathcal{G}\to G/G'$，它由

$$\varphi: x-1\mapsto xG'$$

给出．如果 $\mathcal{G}^2\subseteq\ker\varphi$，则 φ 诱导一个同态 $\mathcal{G}/\mathcal{G}^2\to G/G'$，它显然是 θ' 的逆，这就可以完成证明．

如果 $u\in\mathcal{G}^2$，则

$$\begin{aligned}u &= \Big(\sum_{x\neq 1} m_x(x-1)\Big)\Big(\sum_{y\neq 1} n_y(y-1)\Big)\\ &= \sum_{x,y} m_x n_y (x-1)(y-1)\\ &= \sum_{x,y} m_x n_y((xy-1)-(x-1)-(y-1)).\end{aligned}$$

所以，$\varphi(u)=\prod_{x,y}(xyx^{-1}y^{-1})^{m_x n_y}G'=G'$，因此正如所要的 $u\in\ker\varphi$. ■

群 $H_2(G,\mathbb{Z})$ 是有用的，它叫做 G 的**舒尔乘子**．例如，假设 $G=F/R$，其中 F 是自由群，即有群 G 的一个表现．则**霍普夫公式**是

$$H_2(G,\mathbb{Z})\cong(R\cap F)/[F,R]$$

（见 Rotman 所著的《An Introduction to Homological Algebra》，274 页）．由此群 $(R\cap F)/[F,R]$ 只依赖于 G 而不依赖于 G 的表现的选取．

定义　如果一个正合列 $0\to A\to E\to G\to 1$ 满足 $A\leqslant Z(E)$，则该正合列称为群 G 的**中心扩张**．G 的一个**泛中心扩张**是指一个中心扩张 $0\to M\to U\to G\to 1$，关于它恒存在交换图

$$\begin{array}{ccccccccc}0 & \to & A & \to & E & \to & G & \to & 1\\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle 1_G} & & \\ 0 & \to & M & \to & U & \to & G & \to & 1\end{array}$$

定理　如果 G 是有限群，则 G 有泛中心扩张当且仅当 $G=G'$，此时，$M\cong H_2(G,\mathbb{Z})$，特别地，每个有限单群有泛中心扩张．

证明　见 Milnor 所著的《Introduction to Algebraic K-Theory》，43～46 页． ■

这个定理用来构造单群的"覆盖"．

现在考虑上同调群．

命题 10.111　设 G 是群，设 A 是 G-模，并把 $\mathbb{Z}$ 看作平凡 G-模，则

$$H^0(G,A)=\mathrm{Hom}_G(\mathbb{Z},A)\cong A^G.$$

证明　根据定义，

$$H^0(G,A) = \mathrm{Ext}^0_{\mathbb{Z}G}(\mathbb{Z},A) = \mathrm{Hom}_G(\mathbb{Z},A).$$

定义 $\tau_A:\mathrm{Hom}_G(\mathbb{Z},A)\to A^G$ 为 $f\mapsto f(1)$. 注意 $f(1)\in A^G$：如果 $g\in G$，则 $gf(1)=f(g\cdot 1)$（因为 f 是 G-映射），$g.1=1$（因为 $\mathbb{Z}$ 是 G-平凡的）；所以，$gf(1)=f(1)$，$f(1)\in A^G$. 经简单计算可知 τ_A 是同构． ■

由此，$H^0(G,A)$ 是 A 的最大 G-平凡子模．

定理 10.112　设 $G=\langle\sigma\rangle$ 是有有限阶 k 的循环群，并设 A 是 G-模．如果 $N=\sum_{i=0}^{k-1}\sigma^i$ 和 $D=\sigma-1$，则

$$H^0(G,A)=A^G;$$

$$\text{对一切 } n\geqslant 1, H^{2n-1}(G,A)=\ker N/(\sigma-1)A;$$

$$\text{对一切 } n\geqslant 1, H^{2n}(G,A)=A^G/NA.$$

证明　运用反变函子 $\mathrm{Hom}_G(\ ,A)$ 到引理 10.106 中 $\mathbb{Z}$ 的分解上，注意 $\mathrm{Hom}_G(\mathbb{Z}G,A)\cong A$．现在计算 ker/im 可知有陈述中给出的结果． ■

注意命题 10.103 给出 $\mathrm{im}D=\mathcal{G}A$．

系 10.113　如果 G 是有有限阶 k 的循环群和 A 是平凡 G-模，则

$$H^0(G,A)=A;$$

$$\text{对一切 } n\geqslant 1, H^{2n-1}(G,A)=A[k];$$

$$\text{对一切 } n\geqslant 1, H^{2n}(G,A)=A/kA.$$

特别地，

$$H^0(G,\mathbb{Z})=\mathbb{Z};$$

$$\text{对一切 } n\geqslant 1, H^{2n-1}(G,\mathbb{Z})=\{0\}$$

$$\text{对一切 } n\geqslant 1, H^{2n}(G,\mathbb{Z})=\mathbb{Z}/k\mathbb{Z}.$$

注　一个有限群 G 存在非零整数 d，对一切 $n\geqslant 1$ 和一切 G-模 A 满足

$$H^n(G,A)\cong H^{n+d}(G,A),$$

叫做有**周期上同调**．可以证明群 G 有周期上同调当且仅当它的西罗 p-子群当 p 是奇素数时都是循环群，而它的西罗 2-子群或者是循环群或者是广义四元数（见 Adem-Milgram 所著的《Cohomology of Finite Groups》，148 页）．例如，$G=\mathrm{SL}(2,5)$ 有周期上同调，它是 $120=8\cdot 3\cdot 5$ 阶群，因此它的西罗 3-子群和西罗 5-子群都是循环群，有素数阶，而它的西罗 2-子群同构于四元数．

当 G 未必是循环群时，可以用导子和扩张来说明 $H^1(G,A)$ 和 $H^2(G,A)$，只要能够证明 10.3 节中的那些公式事实上是由 $\mathbb{Z}$ 的投射分解产生．我们需要一个技术性的间歇．

定义　如果 G 是群，定义 $B_0(G)$ 为单一生成元[ ]上的自由 G-模（因此，$B_0(G)\cong\mathbb{Z}G$）且对 $n\geqslant 1$，定义 $B_n(G)$ 为以一切记号 $[x_1\mid x_2\mid\cdots\mid x_n]$ 为基的自由 G-模，其中 $x_i\in G$．定义 $\varepsilon:B_0(G)\to\mathbb{Z}$ 为 $\varepsilon([\,])=1$ 且对 $n\geqslant 1$，定义 $d_n:B_n(G)\to B_{n-1}(G)$ 为

$$d_n:[x_1\mid\cdots\mid x_n]\mapsto x_1[x_2\mid\cdots\mid x_n]$$
$$+\sum_{i=1}^{n-1}(-1)^i[x_1\mid\cdots\mid x_ix_{i+1}\mid\cdots\mid x_n]+(-1)^n[x_1\mid\cdots\mid x_{n-1}].$$

横分解是指序列

$$\mathbf{B}_\bullet(G):\cdots\to B_2(G)\xrightarrow{d_2}B_1(G)\xrightarrow{d_1}B_0(G)\xrightarrow{\varepsilon}\mathbb{Z}\to 0.$$

我们考察横分解的低维部分.

$$d_1: [x] \mapsto x[\,] - [\,];$$

$$d_2: [x \mid y] \mapsto x[y] - [xy] + [x];$$

$$d_3: [x \mid y \mid z] \mapsto x[y \mid z] - [xy \mid z] + [x \mid yz] - [x \mid y]$$

这些公式都是在前面几节中产生的，但没有附加条件 $[x \mid 1] = 0 = [1 \mid y]$ 和 $[1] = 0$. 事实上，有两种横分解；刚才定义的横分解和另一种我们将马上看到的横分解叫做正规化横分解.

横分解是$\mathbb{Z}$的自由分解，虽然不是用简单计算可以证明的；我们把 $\mathbf{B}.(G)$和代数拓扑熟悉的分解相比较，以此证明它是一个分解.

定义 如果 G 是群，设 $P_n(G)$是以 G 的元素的一切 $(n+1)$ 元组为基的自由阿贝尔群；定义

$$x(x_0, x_1, \cdots, x_n) = (xx_0, xx_1, \cdots, xx_n)$$

使 $P_n(G)$成为一个 G-模. 只要 $n \geqslant 1$，定义$\partial_n: P_n(G) \to P_{n-1}(G)$ 为

$$\partial_n: (x_0, x_1, \cdots, x_n) \mapsto \sum_{i=0}^{n} (-1)^i (x_0, \cdots, \hat{x}_i, \cdots, x_n),$$

其中 $\hat{x}_i$ 表示 x_i 已经被删除. $\mathbf{P}.(G)$叫做$\mathbb{Z}$的**齐次分解**.

注意 $P_0(G)$ 是以一切$(y)(y \in G)$ 为基的自由阿贝尔群，由 $x(y) = (xy)$ 做成一个 G-模. 换句话说，$P_0(G) = \mathbb{Z}G$.

证明 $\mathbf{P}.(G)$ 是$\mathbb{Z}$ 的投射分解要分两部分.

引理 10.114 序列

$$\mathbf{P}.(G): \cdots \to P_2(G) \xrightarrow{\partial_2} P_1(G) \xrightarrow{\partial_1} P_0(G) \xrightarrow{\varepsilon} \mathbb{Z} \to 0$$

是一个复形，其中 ε 是增广映射.

证明 只需证明$\partial_{n-1}\partial_n(x_0, x_1, \cdots, x_n) = 0$. 现在

$$\begin{aligned}\partial_{n-1}\partial_n(x_0, x_1, \cdots, x_n) &= \sum_{i=0}^{n} (-1)^i \partial_{n-1}(x_0, \cdots, \hat{x}_i, \cdots, x_n) \\ &= \sum_{i=0}^{n} (-1)^i \Big(\sum_{j<i} (-1)^j (x_0, \cdots, \hat{x}_j, \cdots, \hat{x}_i, \cdots, x_n) \Big) \\ &\quad + \sum_{i=0}^{n} (-1)^i \Big(\sum_{j>i} (-1)^{j-1} (x_0, \cdots, \hat{x}_i, \cdots, \hat{x}_j, \cdots, x_n) \Big).\end{aligned}$$

最后一个等式中，第一个和式的内层有符号$(-1)^j$，这是因为 $j<i$，从而从原始 n 元组中删除 x_i 之后，x_j 仍然在第 j 个位置. 然而，第二个和式的内层符号是$(-1)^{j-1}$，这是因为 $i<j$，从而当 x_i 先被删除之后，x_j 在第 $j-1$ 个位置. 于是，$\partial_{n-1}\partial_n(x_0, x_1, \cdots, x_n)$是$(n-2)$元组$(x_0, \cdots, \hat{x}_i, \cdots, \hat{x}_j, \cdots, x_n)$对 $i<j$ 的和，每一个出现两次；一次由 ∂_n删除 x_i 再由 ∂_{n-1}删除 x_j，第二次由 ∂_n删除 x_j 再由 ∂_{n-1}删除 x_i. 第一种情形中，$(n-2)$元组的符号是$(-1)^{i+j-1}$，第二种情形中，它的符号是$(-1)^{i+j}$. 所以$(n-2)$元组成对抵消，从而 $\partial_{n-1}\partial_n = 0$. ■

命题 10.115 复形

$$\mathbf{P}.(G): \cdots \to P_2(G) \xrightarrow{\partial_2} P_1(G) \xrightarrow{\partial_1} P_0(G) \xrightarrow{\partial_0} \mathbb{Z} \to 0$$

是$\mathbb{Z}$ 的 G-自由分解，其中 $\partial_0 = \varepsilon$ 是增广映射.

证明 我们让读者证明 $P_n(G)$是以形如 $(1, x_1, \cdots, x_n)$ 的一切记号为基的自由 G-模.

为证明 $\mathbf{P}_\bullet(G)$ 的正合性，根据命题 10.40，只需构造一个压缩同伦；即映射

$$\cdots \leftarrow P_2(G) \xleftarrow{s_1} P_1(G) \xleftarrow{s_0} P_0(G) \xleftarrow{s_{-1}} \mathbb{Z}$$

满足 $\varepsilon s_{-1} = 1_{\mathbb{Z}}$ 和

$$对一切\ n \geqslant 0,\ \partial_{n+1} s_n + s_{n-1}\partial_n = 1_{P_n}{}^{(G)}.$$

定义 $s_{-1}: \mathbb{Z} \to P_0(G)$ 为 $m \mapsto m(1)$，其中括号中的 1 是群 G 的幺元，并对 $n \geqslant 0$，定义 $s_n: P_n(G) \to P_{n+1}(G)$ 为

$$s_n: (x_0, x_1, \cdots, x_n) \mapsto (1, x_0, x_1, \cdots, x_n).$$

这些映射 s_n 只是 $\mathbb{Z}$-映射，但习题 10.32 说这已足以证明正合性．下面是计算．

$$\varepsilon s_{-1}(1) = \varepsilon((1)) = 1$$

如果 $n \geqslant 0$，则

$$\begin{aligned}\partial_{n+1} s_n(x_0, \cdots, x_n) &= \partial_{n+1}(1, x_0, \cdots, x_n) \\ &= (x_0, \cdots, x_n) + \sum_{i=0}^{n}(-1)^{i+1}(1, x_0, \cdots, \hat{x}_i, \cdots, x_n)\end{aligned}$$

[求和的范围已经改写，因为 x_i 在 $(1, x_0, \cdots, x_n)$ 中处于第 $(i+1)$ 个位置]．另一方面，

$$\begin{aligned}s_{n-1}\partial_n(x_0, \cdots, x_n) &= s_{n-1}\sum_{j=0}^{n}(-1)^j(x_0, \cdots, \hat{x}_j, \cdots, x_n) \\ &= \sum_{j=0}^{n}(-1)^j(1, x_0, \cdots, \hat{x}_j, \cdots, x_n).\end{aligned}$$ ■

由此 $(\partial_{n+1}s_n + s_{n-1}\partial_n)(x_0, \cdots, x_n) = (x_0, \cdots, x_n)$．

命题 10.116　横分解 $\mathbf{B}_\bullet(G)$ 是 $\mathbb{Z}$ 的 G-自由分解．

证明　对每个 $n \geqslant 0$，定义 $\tau_n: P_n(G) \to B_n(G)$ 为

$$\tau_n: (x_0, \cdots, x_n) \mapsto x_0[x_0^{-1}x_1 \mid x_1^{-1}x_2 \mid \cdots \mid x_{n-1}^{-1}x_n],$$

并定义 $\sigma_n: B_n(G) \to P_n(G)$ 为

$$\sigma_n: [x_1 \mid \cdots \mid x_n] \mapsto (1, x_1, x_1x_2, x_1x_2x_3, \cdots, x_1x_2, \cdots, x_n).$$

容易验证 τ_n 和 σ_n 互逆，因此每个 τ_n 是同构．

读者也可以验证 $\tau: \mathbf{P}_\bullet(\mathbf{G}) \to \mathbf{B}_\bullet(\mathbf{G})$ 是链映射；即下面的图交换：

$$\begin{array}{ccc} P_n(G) & \xrightarrow{\tau_n} & B_n(G) \\ \partial_n\downarrow & & \downarrow d_n \\ P_{n-1}(G) & \xrightarrow{\tau_{n-1}} & B_{n-1}(G) \end{array}$$

最后，习题 10.22 证明两个复形有相同的同调群．根据命题 10.115，复形 $\mathbf{P}_\bullet(G)$ 是正合列，因此它的一切同调群都是 $\{0\}$．由此 $\mathbf{B}_\bullet(G)$ 的一切同调群也都是 $\{0\}$，从而它也是正合列． ■

定义　定义

$$[x_1 \mid \cdots \mid x_n]^* = \begin{cases}[x_1 \mid \cdots \mid x_n] & 如果一切\ x_i \neq 1; \\ 0 & 如果某个\ x_i = 1.\end{cases}$$

正规化横分解 $\mathbf{B}^*_\bullet(\mathbf{G})$ 是指序列

$$\mathbf{B}^*_\bullet(\mathbf{G}): \cdots \to B_2^*(G) \xrightarrow{d_2} B_1^*(G) \xrightarrow{d_1} B_0^*(G) \xrightarrow{\varepsilon} \mathbb{Z} \to 0,$$

其中 $B_n^*(G)$ 是以一切非零 $[x_1 \mid \cdots \mid x_n]^*$ 为基的自由 G-模，映射 d_n 和横分解中的映射有相同的公

式（除了所有符号$[x_1 \mid \cdots \mid x_n]$现在变成$[x_1 \mid \cdots \mid x_n]^*$；特别地，当某个$x_i=1$时，$[x_1]\cdots[x_n]^*=0$）.

因为我们把某些基元素变成了0，所以正规化横分解$\mathbf{B}^*_\bullet(G)$并不显然是一个复形，更不必说$\mathbb{Z}$的分解.

定理 10.117 正规化横分解$\mathbf{B}^*_\bullet(G)$是$\mathbb{Z}$的G-自由分解.

证明 先构造压缩同伦

$$\cdots \leftarrow B_2^*(G) \xleftarrow{t_1} B_1^*(G) \xleftarrow{t_0} B_0^*(G) \xleftarrow{t_{-1}} \mathbb{Z},$$

其中每个t_n是$\mathbb{Z}$-映射. 定义$t_{-1}:\mathbb{Z}\to B_0^*(G)$为$t_{-1}:m\mapsto m[\,]$. 注意，$B_n^*(G)$是以一切非零$[x_1 \mid \cdots \mid x_n]^*$为基的自由$G$-模；因此，它是$\mathbb{Z}G$复制的直和. 因$\mathbb{Z}G$是自由阿贝尔群，$B_n^*(G)$也是自由阿贝尔群；读者可以验证$B_n^*(G)$作为自由阿贝尔群，它的基由一切非零$x[x_1 \mid \cdots \mid x_n]^*$组成. 为了对$n\geqslant 0$定义$t_n$，我们利用$t_n$只需是$\mathbb{Z}$-映射的事实，因此只需给出它在那些$\mathbb{Z}$-基元素上的值（自由性允许我们没有限制地选取这些值）. 于是，对$n\geqslant 0$，定义$t_n:B_n^*(G)\to B_{n+1}^*(G)$为

$$t_n: x[x_1 \mid \cdots \mid x_n]^* \mapsto [x \mid x_1 \mid \cdots \mid x_n]^*.$$

易知我们构造了一个压缩同伦；读者可以验证$\varepsilon t_{-1}=1_{\mathbb{Z}}$和对$n\geqslant 0$，

$$d_{n+1}t_n + t_{n-1}d_n = 1_{B_n^*(G)}.$$

一旦证明了$\mathbf{B}^*_\bullet(G)$是复形就完成了这个证明. 因$\mathbf{B}^*_{n+1}(G)$作为G-模是由$\operatorname{im} t_n$生成的，所以只需证明在这个子群上$d_nd_{n+1}=0$. 现在对$n\geqslant -1$用归纳法证明$d_nd_{n+1}t_n=0$. 基础步为真是因为$\varepsilon=t_{-1}$和$0=\varepsilon d_1=t_{-1}d_1$. 关于归纳步，用压缩同伦定义中的恒等式和归纳假设$d_{n-1}d_n=0$：

$$\begin{aligned}
d_nd_{n+1}t_n &= d_n(1-t_{n-1}d_n) \\
&= d_n - d_nt_{n-1}d_n \\
&= d_n - (1-t_{n-2}d_{n-1})d_n \\
&= d_n - d_n - t_{n-2}d_{n-1}d_n \\
&= 0.
\end{aligned}$$

■

我们现在可以说明$H^1(G,A)$和$H^2(G,A)$.

系 10.118 对每个群G和每个G-模A，10.3节中构造的群$H^1(G,A)$和$H^2(G,A)$和上同调群一致.

证明 我们已经证明了因子组、上边缘、导子和主导子事实上由$\mathbb{Z}$的投射分解形成. ■

命题 10.119 如果G是m阶有限群，则对一切$n\geqslant 1$和一切G-模A，$mH^n(G,A)=\{0\}$.

证明 对$f\in\operatorname{Hom}_G(B_n,A)$，定义$g:B_{n-1}\to A$为

$$g(x_1 \mid \cdots \mid x_{n-1}) = \sum_{y\in G} f(x_1 \mid \cdots \mid x_{n-1} \mid y).$$

和定理10.21的证明一样，对余圈公式求和，在G中对一切$x_{n+1}=y$有

$$\begin{aligned}
(df)(x_1 \mid \cdots \mid x_n \mid x_{n+1}) = {} & x_1 f(x_2 \mid \cdots \mid x_{n+1}) + \sum_{i=1}^{n-2}(-1)^i f(x_1 \mid \cdots \mid x_ix_{i+1} \mid \cdots \mid x_{n+1}) \\
& + (-1)^{n-1}f(x_1 \mid \cdots \mid x_nx_{n+1}) + (-1)^n f(x_1 \mid \cdots \mid x_n).
\end{aligned}$$

在倒数第二项中，因x_{n+1}在G上变化，x_nx_{n+1}也在G上变化. 因此，如果f是余圈，则$df=0$且

$$0 = x_1 g(x_2 \mid \cdots \mid x_{n-1}) + \sum_{i=1}^{n-2}(-i)^i g(x_1 \mid \cdots \mid x_ix_{i+1} \mid \cdots \mid x_n)$$

$$+(-1)^{n-1}g(x_1\mid\cdots\mid x_{n-1})+m(-1)^n f(x_1\mid\cdots\mid x_n)$$

（最后一项与 x_{n+1} 无关）．因此，

$$0=dg+(-1)^n mf,$$

从而 mf 是上边缘．■

系 10.120　*如果 G 是有限群和 A 是有限生成 G-模，则对一切 $n\geqslant 0$，$H^n(G,A)$ 是有限的．*

证明　$H^n(G,A)$ 是有限生成的指数有限的阿贝尔群（因为 A 是有限生成的）．■

命题 10.119 和它的系对同调群也成立．

群的上同调还有几个方面我们没有提到．除了在群论中是一个有用的工具之外，这些群形成了和代数拓扑的联系．对每个群 G，存在一个拓扑空间 $K(G,1)$ 叫做艾伦伯格-麦克莱恩空间，它的基本群是 G，它的上同调群和代数定义的上同调群一致．[⊖] 事实上，在群论和代数拓扑之间存在更深刻的联系，这只是第一个信号．

群的上同调的一个重要性质是一个群的上同调和它的子群及商群的上同调之间的关系．如果 $\varphi: S\to G$ 是同态，如果对一切 $s\in S$ 和 $a\in A$ 定义 $sa=\varphi(s)a$，则每个 G-模 A 变成一个 S-模．$H^n(S,A)$ 和 $H^n(G,A)$ 之间有什么联系？$H_n(S,A)$ 和 $H_n(G,A)$ 之间有什么联系？[同调群和上同调群之间还有一个联系：$H^n(G,A)^*\cong H_n(G,A^*)$，其中 $A^*=\mathrm{Hom}_{\mathbb{Z}}(A,\mathbb{Q}/\mathbb{Z})$．]

有三个标准映射，我们将用横分解来定义．第一个是**限制**．如果 S 是群 G 的子群，则每个函数 $f: B_n(G)\to A$ 都是定义在一切 $[x_1\mid\cdots\mid x_n]$ 上的，其中 $x_i\in G$；当然，f 在一切形如 $[s_1\mid\cdots\mid s_n]$ 的 n 元组上有定义，其中 $s_i\in S\subseteq G$，因此它的限制是 $B_n(S)\to A$ 的映射，记为 $f\mid S$．如果 f 是一个 n-余圈，我们用 $\mathrm{cls}f$ 记它的上同调类：$\mathrm{cls}f=f+\mathrm{im}\,d_{n+1}$．定义

$$\mathrm{Res}: H^n(G,A)\to H^n(S,A)$$

为 $\mathrm{Res}(\mathrm{cls}f)=\mathrm{cls}(f\mid s)$．有一个结果，如果 G 是有限群，S_p 是西罗 p-子群，$n\geqslant 1$，则 $\mathrm{Res}: H^n(G,A)\to H^n(S_p,A)$ 是 $H^n(G,A)$ 的 p-准素分量上的单射；于是 G 的上同调受到它的西罗子群的上同调的很大影响．

如果 $S\leqslant G$，有一个反方向的映射

$$\mathrm{Cor}: H^n(S,A)\to H^n(G,A)$$

叫做**余限制**，当 S 在 G 中有有限指数时这个映射有定义．我们先在 0 维中定义 Cor，即定义 $\mathrm{Cor}^0: A^S\to A^G$ 为 $a\mapsto\sum_{t\in T}ta$，其中 T 是 S 在 G 中的一个左陪集代表系（当然，我们必须验证 Cor^0 是不依赖于陪集代表系选取的同态）．把 0 维中的映射扩张到高维中的映射有一个标准的方法（本质上是长度推移法），且如果 $[G:S]=m$，则

$$\mathrm{Cor}^n\circ\mathrm{Res}^n: H^n(G,A)\to H^n(G,A)=m;$$

即复合是乘 m．类似地，在同调中，定义为 $a+\mathcal{G}A\mapsto\sum_{t\in T}t^{-1}a+\mathcal{S}A$ 的映射

$$\mathrm{Cor}_0: A/\mathcal{G}A\to A/\mathcal{S}A$$

可以扩张为高维中的映射．当 $n=1$ 和 $A=\mathbb{Z}$ 时，有 $\mathrm{Cor}_1: H_1(G,\mathbb{Z})\to H_1(S,\mathbb{Z})$；即 $\mathrm{Cor}_1: G/G'\to S/S'$．有一个群论家熟知的叫做**转移** $V_{G\to S}$ 的同态，由此，$\mathrm{Cor}_1=V_{G\to S}$．

第三个标准映射叫做**提升**．假设 N 是群 G 的正规子群．如果 A 是 G-模，并对 $a\in A^N$ 定义

⊖ 由于这种拓扑联系，许多作者用记号 $H^n(\pi,\mathbb{Z})$ 表示上同调群，因为 π_1 是基本群的标准记号．

$(gN)a = ga$，则 A^N 是 G/N-模［如果 $gN = hN$，则有某个 $x\in N$ 使得 $h=gx$，因 $xa=a$，从而 $ha=(gx)a=g(xa)=ga$］. 定义

$$\mathrm{Inf}: H^n(G/N,A^N) \to H^n(G,A)$$

为 $\mathrm{cls}f\mapsto \mathrm{cls}(f^{\#})$，其中

$$f^{\#}:[g_1 \mid \cdots \mid g_n]\mapsto f[g_1N \mid \cdots \mid g_nN].$$

这里一个有用的结果是**五项正合列**：如果 $N\lhd G$ 和 A 是 G-模，则存在阿贝尔群的正合列

$$0 \to H^1(G/N,A^N) \xrightarrow{\mathrm{Inf}} H^1(G,A) \xrightarrow{\mathrm{Res}} H^1(N,A)^{G/N} \longrightarrow H^2(G/N,A^N) \longrightarrow H^2(G,A)$$

（在同调中也有类似序列）. 关于这些思想的一个极好的讨论，读者可参考 Serre 所著的《Corps Locaux》，135～138 页 .

我们可以在 $H^{\bullet}(G,R)=\sum_{n\geqslant 0}H^n(G,R)$ 上（其中 R 是任意交换环）定义上积迫使上同调群成为一个分次环（见 Evens 所著的《The Cohomology of Groups》），这个附加的结构有重要应用 .

我们现在考虑自由群的上同调 .

引理 10.121 *如果 G 是以 X 为基的自由群，则它的增广理想$\mathcal{G}$是以*

$$X-1=\{x-1: x\in X\}$$

为基的自由 G-模 .

证明 我们先证明$\mathcal{G}$由一切 $X-1$ 生成 . 恒等式

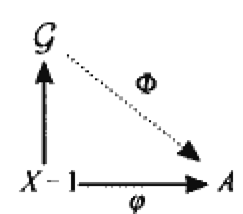
$$xy-1=(x-1)+x(y-1)$$

和

$$x^{-1}-1=-x^{-1}(x-1)$$

表明，如果 w 是 X 中的任一字，则 $w-1$ 可以写成 $X-1$ 的 G-线性组合 .

为证明$\mathcal{G}$是以 $X-1$ 为基的自由 G-模，根据命题 7.49，只需证明能够完成下面的图：



其中 A 是任意 G-模和 φ 是任意函数（这样的映射 Φ 的唯一性来自 $X-1$ 生成$\mathcal{G}$）. 于是，我们寻找 $\Phi\in \mathrm{Hom}_G(\mathcal{G},A)$. 根据习题 10.59，经 $f: x\mapsto f(x-1)$（其中 $f\in\mathcal{G}\to A$）有 $\mathrm{Hom}_G(\mathcal{G},A)\cong \mathrm{Der}(G,A)$，因此我们找到一个导子 .

考虑（必分裂）扩张 $0\to A\to E\to G\to 1$，可知 E 由一切有序对 $(a,g)\in A\times G$ 组成 . 给定的函数 $\varphi: X-1\to A$ 定义了 G 的生成集 X 的一个提升 ℓ，就是

$$\ell(x)=(\varphi(x-1),x).$$

因 G 是以 X 为基的自由群，函数 $\ell: X\to E$ 可以扩张为同态 $L: G\to E$. 我们断言，对每个 $g\in G$，$L(g)=(d(g),g)$，其中 $d: G\to A$. 每个 $g\in G$ 作为约化字有唯一的表达式 $g=x_1^{e_1}\cdots x_n^{e_n}$，其中 $x_i\in X$ 和 $e_i=\pm 1$. 我们对 $n\geqslant 1$ 用归纳法证明这个断言 . 基础步是显然的，而

$$\begin{aligned} L(g) &= L(x_1^{e_1}\cdots x_n^{e_n}) \\ &= L(x_1^{e_1})\cdots L(x_n^{e_n}) \\ &= (\varphi(x_1-1),x_1)^{e_1}\cdots(\varphi(x_n-1),x_n)^{e_n} \\ &= (d(g),g), \end{aligned}$$

因此第一个坐标 $d(g)$在 A 中．最后，因为 L 是同态，所以 d 是一个导子.

现在习题 10.59 说对一切 $g\in G$ 存在定义为 $\Phi(g-1)=d(g)$ 的同态 $\Phi:\mathcal{G}\to A$. 特别地，$\Phi(x-1)=d(x)=\varphi(x-1)$，因此 Φ 扩张 φ. ■

定理 10.122　*如果 G 是自由群，则对一切 $n>1$ 和一切 G-模 A，$H^n(G,A)=\{0\}$.*

证明　序列 $0\to\mathcal{G}\to \mathbb{Z}G\to\mathbb{Z}\to 0$ 是$\mathbb{Z}$的自由分解，这是因为$\mathcal{G}$现在是自由 G-模．于是，在删除分解中非零项只出现在 0 和 1 的位置，因此对 $n>1$ 一切上同调群消失． ■

我们现在要陈述一个重要结果（Stallings-Swan 定理)，它是用同调的方法发现的，但是在它的陈述中没有提到同调．

如果 G 是群且 $S\leqslant G$ 是子群，则每个 G-模 A 可以看作一个 S-模，这是因为$\mathbb{Z}S$是$\mathbb{Z}G$的子环．

定义　*如果群 G 对一切G-模 A 和 G 的每个子群 S 有*

$$H^{n+1}(S,A)=\{0\},$$

*则称 G 的***上同调维数***$\leqslant n$，用记号表示为 $\mathrm{cd}(G)\leqslant n$. 如果这样的整数 n 不存在，则记为$\mathrm{cd}(G)=\infty$.*

我们说 $\mathrm{cd}(G)=n$ 如果 $\mathrm{cd}(G)\leqslant n$ 但 $\mathrm{cd}(G)\leqslant n-1$不成立．

例 10.123　(i) 如果 $G=\{1\}$，则 $\mathrm{cd}(G)=0$；这是因为 G 是 1 阶循环群，从而可由定理 10.112 推出结果．

(ii) 假设 G 是无限循环群．因为每个子群 $S\subseteq G$ 都是循环群，所以定理 10.122 给出$d(G)\leqslant 1$. 如果 $d(G)=0$,则 $H^1(S,A)=\{0\}$对一切子群 S 和一切模 A 成立．特别地，如果$S\cong\mathbb{Z}$和 $A\neq\{0\}$是平凡模，则 $H^1(S,A)=\mathrm{Der}(S,A)/\mathrm{PDer}(S,A)\cong\mathrm{Hom}(\mathbb{Z},A)\neq\{0\}$. 因此，$d(G)=1$.

如果 G 是阶 $k>1$ 的有限循环群，则 cd $(G)=\infty$，如同我们在系 10.113 中看到的那样，其中 $A=\mathbb{Z}$.

(iii) 如果 $G\neq\{1\}$是自由群，则定理 10.122 证明 $\mathrm{cd}(G)=1$，这是因为自由群的每个子群也是自由的．

(iv) 如果 $\mathrm{cd}(G)<\infty$，则 G 必是无挠的；否则，G 有有限阶 $k>1$ 的循环子群 S，且对一切偶数 n, $H^n(S,\mathbb{Z})\neq 0$.

(v) 如果 G 是有有限秩 n 的自由阿贝尔群，则 $\mathrm{cd}(G)=n$. ■

命题 10.124（沙皮罗引理）　*设 G 是群，并设 $S\leqslant G$ 是子群．如果 A 是$\mathbb{Z}S$-模，则对一切$n\geqslant 0$,*

$$H^n(S,A)\cong H^n(G,\mathrm{Hom}_{\mathbb{Z}S}(\mathbb{Z}G,A)).$$

证明　设$\cdots\to P_1\to P_0\to\mathbb{Z}\to 0$ 是$\mathbb{Z}G$-自由分解．如果记 $\mathrm{Hom}_{\mathbb{Z}S}(\mathbb{Z}G,A)$为 A^*，则

$$H^n(G,A^*)=H^n(\mathrm{Hom}_{\mathbb{Z}G}(\mathbf{P}_\bullet,A^*)).$$

根据伴随同构，

$$\begin{aligned} \mathrm{Hom}_{\mathbb{Z}G}(P_i,A^*) &= \mathrm{Hom}_{\mathbb{Z}G}(P_i,\mathrm{Hom}_{\mathbb{Z}S}(\mathbb{Z}G,A)) \\ &\cong \mathrm{Hom}_{\mathbb{Z}S}(P_i\otimes_{\mathbb{Z}G}\mathbb{Z}G,A) \\ &\cong \mathrm{Hom}_{\mathbb{Z}S}(P_i,A). \end{aligned}$$

但引理8.141(i)（的证明）表明$\mathbb{Z}G$是自由$\mathbb{Z}S$-模，因此自由$\mathbb{Z}G$-模 P_i 也是自由$\mathbb{Z}S$-模．由此可以

把 **P.** 看作Z 的ZS-自由分解，并存在复形的同构：

$$\mathrm{Hom}_{ZS}(\mathbf{P}_\bullet, A) \cong \mathrm{Hom}_{ZG}(\mathbf{P}_\bullet, A^*).$$

因此，它们的同调群同构；即 $H^n(S,A) \cong H^n(G,A^*)$. ■

系 10.125 如果 G 是群和 $S \leqslant G$ 是子群，则

$$\mathrm{cd}(S) \leqslant \mathrm{cd}(G).$$

证明 可以假定 $\mathrm{cd}(G)=n<\infty$. 如果 $m>n$ 且存在ZS-模 A 使得 $H^m(S,A)\neq\{0\}$，则沙皮罗(Shapiro)引理给出 $H^m(G,\mathrm{Hom}_{ZS}(ZG,A))\cong H^m(S,A)\neq\{0\}$，与 $\mathrm{cd}(G)=n$ 矛盾. ■

系 10.126 有有限上同调维数的群 G 没有（除 1 之外的）有限阶元素.

证明 由例10.123(ii)和上面的系立得. ■

存在不自由的群 G 使得 $\mathrm{cd}(G)=1$吗？Stallings 证明了下面的漂亮定理（F_2G 表示F_2 上的群代数）.

定理 如果 G 是有限表现群，且 $H^1(G,F_2G)$的元素多于 2 个，则 G 是自由积，$G=H*K$，其中 $H\neq\{1\}$和 $K\neq\{1\}$（自由积是 **Groups** 中的余积）.

作为一个推论，他证明了下面的结果.

系 如果 G 是有限生成群，且 $\mathrm{cd}(G)=1$，则 G 是自由的.

系 如果 G 是无挠的有限生成群，且有一个指数有限的自由子群，则 G 是自由群.

R. G. Swan 证明上面两个系中去掉 G 是有限生成的假设仍然为真.

定理（Stallings-Swan） 具有有限指数的自由子群的无挠群必是自由群.

系 10.127 群 $G=\{1\}$当且仅当 $\mathrm{cd}(G)=0$.

证明 如果 $G=\{1\}$，则由例10.123(i)，$\mathrm{cd}(G)=0$. 反之，如果 $\mathrm{cd}(G)=0$，则对 G 的每个循环子群 S，$\mathrm{cd}(S)=0$. 根据例10.122(ii)和10.122(iii)可知，一切 $S=\{1\}$,因此 $G=\{1\}$. ■

对这些定理的证明读者可参考 D. E. Cohen 所著的《Groups of Cohomological Dimension1》，Lecture Notes in Mathematics，Vol. 245，Springer-Verlag，New York，1972.

习题

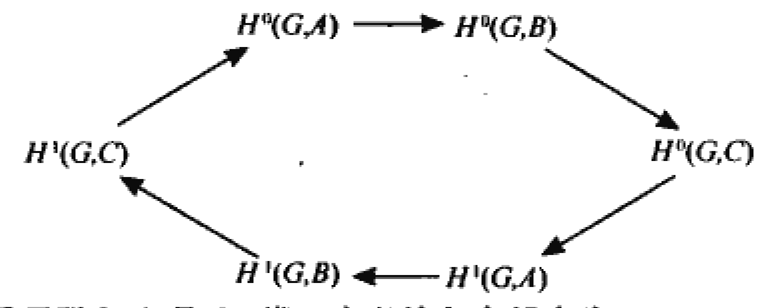
10.58 (i) 证明命题 10.104 中的同构构成Z $\otimes_G$ 和 $A \mapsto A/\mathcal{G}A$ 的自然等价.

(ii) 证明命题 10.111 中的同构构成 $\mathrm{Hom}_G(\mathrm{Z}, \ )$ 和 $A \mapsto A^G$ 的自然等价.

10.59 对固定的群 G，证明函子 $\mathrm{Hom}_G(\mathcal{G}, \ )$ 和 $\mathrm{Der}(G, \ )$ 自然等价.

提示：如果 $f: \mathcal{G} \to A$ 是同构，则 $d_f: x \mapsto f(x-1)$ 是导子.

10.60 (i) 如果 G 是有限循环群和 $0 \to A \to B \to C \to 0$ 是 G-模的正合列，证明存在正合六边形；即在图的每个顶点有核=象. 注意这个习题是类域论中的一个关键引理.



(ii) 如果 G 是有限循环群和 A 是 G-模，定义埃尔布朗商为

$$h(A) = |H^0(G,A)| / |H^1(G,A)|$$

[只有当 $H^0(G,A)$ 和 $H^1(G,A)$ 都有限时，$h(A)$ 才有定义]. 设 $0\to A\to B\to C\to 0$ 是 G-模的正合列．证明：如果埃尔布朗商对模 A，B，C 中的两个有定义，则对第三个也有定义，且

$$h(B)=h(A)h(C).$$

10.61　如果 G 是群，证明

$$P_n(G)\cong\bigotimes_1^{n+1}\mathbb{Z}G,$$

其中 $P_n(G)$ 是齐次分解 $\mathbf{P}_\bullet(G)$ 中的第 n 项，且

$$\bigotimes_1^n\mathbb{Z}G=\mathbb{Z}G\otimes_\mathbb{Z}\mathbb{Z}G\otimes_\mathbb{Z}\cdots\otimes_\mathbb{Z}\mathbb{Z}G,$$

即 n 个 $\mathbb{Z}G$ 在 $\mathbb{Z}$ 上的张量积．

10.62　如果 G 是有限循环群，证明对一切 G-模 A 和一切 $n\geqslant 1$，$H^n(G,A)\cong H_{n+1}(G,A)$.

10.63　设 G 是群．

（ⅰ）对任意阿贝尔群 A，证明 $A^*=\mathrm{Hom}_\mathbb{Z}(\mathbb{Z}G,A)$ 是左 $\mathbb{Z}G$-模．我们称 A^* 为**余诱导模**．

提示：如果 $\varphi:\mathbb{Z}G\to A$ 和 $g\in G$，定义 $g\varphi$ 为 $x\mapsto g\varphi(g^{-1}x)$.

（ⅱ）对任意左 $\mathbb{Z}G$-模 B，证明 $\mathrm{Hom}_{\mathbb{Z}G}(B,A^*)\cong\mathrm{Hom}_\mathbb{Z}(B,A)$.

提示：用伴随同构，即定理 8.99.

（ⅲ）如果 A^* 是余诱导模，证明对一切 $n\geqslant 1, H^n(G,A^*)=\{0\}$.

10.64　如果 G 是群和 A 是阿贝尔群，称 $\mathbb{Z}G$-模 $A_*\mathbb{Z}G\otimes_\mathbb{Z}A$ 为**诱导模**．证明对一切 $n\geqslant 1$，$H_n(G,A_*)=\{0\}$.

10.8　叉积

本节本质上是描述性的，表明如何用上同调群来研究除环．我们先回到伽罗瓦理论．

定理 10.128　*设 E/k 是伽罗瓦扩张，它有伽罗瓦群 $G=\mathrm{Gal}(E/k)$. 乘法群 $E^\times$ 是 kG-模，且*

$$H^1(G,E^\times)=\{0\}.$$

证明　如果 $c:G\to E^\times$ 是 1-余圈，记 $c(\sigma)$ 为 c_σ. 在乘法记号中，余圈条件是对一切 σ，$\tau\in G$ 有恒等式 $\sigma(c_\tau)c_{\sigma\tau}^{-1}c_\sigma=1$；即

$$\sigma(c_\tau)=c_{\sigma\tau}c_\sigma^{-1}.\tag{1}$$

对 $e\in E^\times$，考虑

$$b=\sum_{\tau\in G}c_\tau\tau(e).$$

根据特征标的无关性，即命题 4.30，存在某个 $e\in E^\times$ 使得 $b\neq 0$. 对这样的元素 e，运用等式(1)有

$$\begin{aligned}\sigma(b)&=\sum_{\tau\in G}\sigma(c_\tau)\sigma\tau(e)\\&=\sum_{\tau\in G}c_{\sigma\tau}c_\sigma^{-1}\sigma\tau(e)\\&=c_\sigma^{-1}\sum_{\tau\in G}c_{\sigma\tau}\sigma\tau(e)\\&=c_\sigma^{-1}\sum_{\omega\in G}c_\omega\omega(e)\\&=c_\sigma^{-1}b.\end{aligned}$$

因此，$c_\sigma=b\sigma(b)^{-1}$，从而 c 是上边缘．所以 $H^1(G,E^\times)=\{0\}$.　■

定理 10.128 蕴涵定理 4.50，该定理描述了在一个循环扩张中范数为 1 的元素．

系 10.129（希尔伯特定理 90） 设 E/k 是伽罗瓦扩张，它的伽罗瓦群 $G=\mathrm{Gal}(E/k)$ 是循环群，比如有生成元 σ. 如果 $u\in E^\times$，则 $Nu=1$ 当且仅当存在 $v\in E^\times$ 使得

$$u=\sigma(v)v^{-1}.$$

证明 根据定理 10.112，有 $H^1(G,E^\times)=\ker N/\mathrm{im}D$，其中 N 是范数（记住 $E^\times$ 是乘法群）和 $De=\sigma(e)e^{-1}$．定理 10.128 给出 $H^1(G,E^\times)=\{0\}$，从而 $\ker N=\mathrm{im}D$. 因此，如果 $u\in E^\times$，则 $Nu=1$ 当且仅当存在 $v\in E^\times$ 使得 $u=\sigma(v)v^{-1}$. ■

定理 10.128 是叫做伽罗瓦上同调的最初结果之一．另一个较早的结果是对一切 $n\geqslant 1$，$H^n(G,E)=\{0\}$，其中 E(和 $E^\times$ 对照）是伽罗瓦扩张的加法群（这个结果容易从正规基定理得到). 我们现在要证明 $H^2(G,E^\times)$在除环研究中是有用的．

在本文中只给出了一个非交换除环的例子：四元数$\mathbb{H}$（这是一个$\mathbb{R}$-代数）以及对每个子域$k\subseteq\mathbb{R}$，它的 k-代数的类似物（事实上，习题 9.80 给出了另一个例子）．哈密顿在 1843 年发现四元数，弗罗贝尼乌斯在 1880 年证明$\mathbb{R}$-可除代数只有$\mathbb{R}$，$\mathbb{C}$ 和$\mathbb{H}$（见定理 9.124）．直到 20 世纪初韦德伯恩和迪克森发现循环代数之前，我们不知道还有其他非交换除环的例子．1932 年，阿尔伯特找到一个不是循环代数的叉积代数的例子，1972 年，阿米苏尔找到一个不是叉积代数的非交换除环的例子．

韦德伯恩证明每个有限除环是域（见定理 8.23）．存在特征为素数的除环吗？

我们从初等计算开始．假设 V 是域 E 上的向量空间，它有基 $\{u_\sigma:\sigma\in G\}$，其中 G 是某个集合，从而每个 $v\in V$ 作为 E-线性组合有唯一的表达式 $v=\sum_\sigma a_\sigma u_\sigma$，其中 $a_\sigma\in E$. 对函数 $\mu:V\times V\to V$，记 $\mu(u_\sigma,u_\tau)$ 为 $u_\sigma u_\tau$，定义**结构常数** $g_\alpha^{\sigma,\tau}\in E$ 为

$$u_\sigma u_\tau=\sum_{\sigma\in G}g_\alpha^{\sigma,\tau}u_\alpha.$$

为了满足结合律，必须有 $u_\sigma(u_\tau u_\omega)=(u_\sigma u_\tau)u_\omega$；展开这个等式，每个 u_β 的系数是

$$\sum_\alpha g_\alpha^{\sigma,\tau}g_\beta^{\alpha,\omega}=\sum_\gamma g_\gamma^{\tau,\omega}g_\beta^{\sigma,\gamma}.$$

（爱因斯坦和式约定Σ不使用重叠指标，以使公式变得清晰.）

我们化简这些等式．设 G 是群，并假设 $g_\alpha^{\sigma,\tau}=0$ 除非 $\alpha=\sigma\tau$; 即 $u_\sigma u_\tau=f(\sigma,\tau)u_{\sigma\tau}$，其中 $f(\sigma,\tau)=g_{\sigma\tau}^{\sigma,\tau}$. 函数 $f:G\times G\to E^\times$ 由 $f(\sigma,\tau)=g_{\sigma\tau}^{\sigma,\tau}$ 给出，对一切 $\sigma,\tau,\omega\in G$，它满足下面等式：

$$f(\sigma,\tau)f(\sigma\tau,\omega)=f(\tau,\omega)f(\sigma,\tau\omega),$$

这个等式使人回想起用乘法记号写出的余圈恒等式．这就是为什么在下一定义中要加入因子组．

设 E/k 是伽罗瓦扩张，且 $\mathrm{Gal}(E/k)=G$，又设 $f:G\times G\to E^\times$ 是一个因子组：用乘法记号为

$$对一切\ \sigma,\tau\in G,f(\sigma,1)=1=f(1,\tau),$$

如果记 $\sigma\in G$ 在 $a\in E^\times$ 上的作用为 a^σ，则

$$f(\sigma,\tau)f(\sigma\tau,\omega)=f(\tau,\omega)^\sigma f(\sigma,\tau\omega).$$

定义 给定伽罗瓦扩张 E/k，它有伽罗瓦群 $G=\mathrm{Gal}(E/k)$，以及一个因子组 $f:G\times G\to E^\times$，定义**叉积代数**(E,G,f)为 E 上以一切记号 $\{u_\sigma:\sigma\in G\}$ 为基的向量空间，且有乘法：对一切a，$b\in E$，

$$(au_\sigma)(bu_\tau)=ab^\sigma f(\sigma,\tau)u_{\sigma\tau}.$$

如果 G 是循环群，则称叉积代数(E,G,f)为**循环代数**．

因(E,G,f)中的每个元素有形如$\sum a_\sigma u_\sigma$ 的唯一表达式，乘法的定义由线性扩张到(E,G,f)的一切元素．我们注意两个特殊情形：

$$u_\sigma b = b^\sigma u_\sigma;$$
$$u_\sigma u_\tau = f(\sigma,\tau)u_{\sigma\tau}.$$

命题 10.130 如果 E/k 是伽罗瓦扩张，它有伽罗瓦群 $G=\mathrm{Gal}(E/k)$，又如果 $f: G\times G\to E^\times$ 是因子组，则(E,G,f)是中心单 k-代数，它被 E 分裂．

证明 记(E,G,f)为 A. 首先，我们证明 A 是 k 代数．为证明 A 是结合的，只需证明

$$au_\sigma(bu_\tau cu_\omega) = (au_\sigma bu_\tau)cu_\omega,$$

其中 a，b，$c\in E$. 用乘法定义，

$$\begin{aligned}au_\sigma(bu_\tau cu_\omega) &= au_\sigma(bc^\tau f(\tau,\omega)u_{\tau\omega})\\ &= a(bc^\tau f(\tau,\omega))^\sigma f(\sigma,\tau\omega)u_{\sigma\tau\omega}\\ &= ab^\sigma c^{\sigma\tau}f(\tau,\omega)^\sigma f(\sigma,\tau\omega)u_{\sigma\tau\omega}.\end{aligned}$$

还有

$$\begin{aligned}(au_\sigma bu_\tau)cu_\omega &= ab^\sigma f(\sigma,\tau)u_{\sigma\tau}cu_\omega\\ &= ab^\sigma f(\sigma,\tau)c^{\sigma\tau}f(\sigma\tau,\omega)u_{\sigma\tau\omega}\\ &= ab^\sigma c^{\sigma\tau}f(\sigma,\tau)f(\sigma\tau,\omega)u_{\sigma\tau\omega}.\end{aligned}$$

余圈恒等式表明 A 中的乘法是结合的．

u_1 是 A 中的幺元来自因子组是正规化的假定：

$$u_1u_\tau = f(1,\tau)u_{1\tau} = u_\tau \text{ 和 } u_\sigma u_1 = f(\sigma,1)u_{\sigma 1} = u_\sigma.$$

我们已经证明 A 是环．我们断言 $ku_1=\{au_1: a\in k\}$ 是中心 $Z(A)$. 如果 $a\in E$，则 $u_\sigma au_1=a^\sigma u_\sigma$. 如果 $a\in k=E^G$，则对一切 $\sigma\in G, a^\sigma=a$，因此 $k\subseteq Z(A)$. 关于反包含，假设 $z=\sum_\sigma a_\sigma u_\sigma\in Z(A)$. 对任意 $b\in E$，有 $zbu_1=bu_1z$. 但

$$zbu_1 = \sum a_\sigma u_\sigma bu_1 = \sum a_\sigma b^\sigma u_\sigma.$$

另一方面，

$$bu_1z = \sum ba_\sigma u_\sigma.$$

对每个 $\sigma\in G$，有 $a_\sigma b^\sigma=ba_\sigma$，因此，如果 $a_\sigma\neq 0$，则 $b^\sigma=b$. 如果 $\sigma\neq 1$ 和 $H=\langle\sigma\rangle$ 则根据定理 4.33，$E^H\neq E^{\{1\}}=E$，从而存在 $b\in E$ 使得 $b^\sigma\neq b$. 由此可知$z=a_1u_1$. 对每个 $\sigma\in G$，等式$(a_1u_1)u_\sigma=u_\sigma(a_1u_1)$给出 $a_1^\sigma=a_1$，因此 $a_1\in E^G=k$. 所以 $Z(A)=ku_1$.

我们现在证明 A 是单的．首先注意到每个 u_σ 都是可逆的，这是因为它的逆是 $f(\sigma^{-1},\sigma)^{-1}u_{\sigma^{-1}}$（记住 $\mathrm{im} f\subseteq E^\times$，从而它的值是非零的）．设 I 是 A 中的非零双边理想，并选取一个长度最短的非零 $y=\sum_\sigma c_\sigma u_\sigma\in I$，即 y 有最少个数的非零系数．如有必要，乘以 $(c_\sigma u_\sigma)^{-1}$，从而可以假定 $y=u_1+c_\tau u_\tau+\cdots$. 假设 $c_\tau\neq 0$. 因 $\tau\neq 1_E$，所以存在 $a\in E$ 使得 $a^\tau\neq a$. 现在 I 包含 $ay-ya=b_\tau u_\tau+\cdots$，其中 $b_\tau=c_\tau(a-a^\tau)\neq 0$. 因此 I 包含 $y-c_\tau b_\tau^{-1}(ay-ya)$，它比 y 短（它包含 u_1 但不包含 u_τ）．由此可知 y 的长度必为 1，即 $y=c_\sigma u_\sigma$．但 y 是可逆的，所以 $I=A$. 因此 A 是单的．

最后，定理 9.127 说 A 被 K 分裂，其中 K 是 A 的任意极大子域．读者可以用引理 9.117 证明 $Eu_1\cong E$ 是一个极大子域． ■

根据命题 10.130，自然期望在相对布饶尔群和上同调之间有某种联系．

定理 设 E/k 是伽罗瓦扩张，且 $G=\mathrm{Gal}(E/k)$. 存在经 $\mathrm{cls}f\mapsto[(G,E,f)]$ 的同构

$H^2(G,E^\times)\to\text{Br}(E/k)$.

证明概要 通常这个定理的证明相当长．下列每个项目：同构是合理定义的函数；它是同态；它是单射；它是满射，必须都要验证，且证明是计算性的．例如，Herstein 所著的《Noncommutative Rings》中的证明从 110～116 页．在 Serre 所著的《Corps Locaux》164～167 页中有一个计算较少的证明，用了下降的方法． ■

这个同构的好处是什么？在系 9.132 中，我们看到

$$\text{Br}(k)=\bigcup_{E/k\text{有限}}\text{Br}(E/k).$$

系 10.131 *设 k 是域．*

（ⅰ）布饶尔群 $\text{Br}(k)$ 是挠群．

（ⅱ）如果 A 是中心单 k-代数，则存在整数 n 使得 r 个（r 是 $[A]$ 在 $\text{Br}(k)$ 中的阶）A 的张量积是一个矩阵代数：

$$A\otimes_k A\otimes_k\cdots\otimes_k A\cong\text{Mat}_n(k).$$

证明概要 （ⅰ）$\text{Br}(k)$ 是相对布饶尔群 $\text{Br}(E/k)$ 的并，其中 E/k 是有限的．可以证明 $\text{Br}(k)$ 是这种 $\text{Br}(E/k)$ 的并，其中 E/k 是伽罗瓦扩张．我们现在可以调用命题 10.119，它说 $|G|\,H^2(G,E^\times)=\{0\}$.

（ⅱ）张量积是布饶尔群中的二元运算． ■

回忆命题 9.129：存在域 k 上的非交换可除 k-代数当且仅当 $\text{Br}(k)\neq\{0\}$.

系 10.132 *设 k 是域．如果存在循环伽罗瓦扩张 E/k 满足范数 $N:E^\times\to k^\times$ 不是满射，则存在非交换 k-可除代数．*

证明概要 如果 G 是有限循环群，则定理 10.112 给出

$$H^2(G,E^\times)=(E^\times)^G/\text{im}N=k^\times/\text{im}N.$$

所以，如果 N 不是满射，则 $\text{Br}(E/k)\neq\{0\}$，这蕴涵 $\text{Br}(k)\neq\{0\}$. ■

如果 k 是有限域和 E/k 是有限扩张，则根据有限除环上的韦德伯恩定理（定理 8.23），范数 $N:E^\times\to k^\times$ 是满射．

系 10.133 *如果 p 是素数，则存在特征为 p 的非交换可除代数．*

证明 如果 k 是特征为 p 的域，只需找到一个循环扩张 E/k，对于它范数 $N:E^\times\to k^\times$ 不是满射；即要寻找不是范数的某个 $z\in k^\times$.

如果 p 是奇素数，设 $k=\mathbb{F}_p(x)$. 因 p 是奇数，t^2-x 是可分不可约多项式，从而 $E=k(\sqrt{x})$ 是次数为 2 的伽罗瓦扩张．如果 $u\in E$，则存在多项式 a，b，$c\in\mathbb{F}_p[x]$ 使得 $u=(a+b\sqrt{x})/c$. 此外，

$$N(u)=(a^2-b^2x)/c^2.$$

我们断言 x^2+x 不是范数．否则，

$$a^2-b^2x=c^2(x^2+x).$$

因 $c\neq0$，多项式 $c^2(x^2+x)\neq0$，且次数是偶数．另一方面，如果 $b\neq0$，则 a^2-b^2x 的次数为奇数，这是一个矛盾．如果 $b=0$，则 $u=a/c$；因 $a^2=c^2(x^2+x)$，有 $c^2\mid a^2$，因此 $c\mid a$，从而 $u\in\mathbb{F}_p[x]$ 是多项式．但易知 x^2+x 不是一个多项式的平方．由此可知 $N:E^\times\to k^\times$ 不是满射．

这里有一个特征为 2 的例子．设 $k=\mathbb{F}_2(x)$，并设 $E=k(\alpha)$，其中 α 是 $f(t)=t^2+t+x+1$ 的一个根［$f(t)$ 是不可约的和可分的；它的另一个的根是 $\alpha+1$］．和以前一样，每个 $u\in E$ 可以写成

$u=(a+b\alpha)/c$ 的形式，其中 $a,b,c\in \mathbb{F}_2[x]$. 当然，可以假定 x 不是三个多项式 a，b 和 c 中任一个的因式．此外，

$$N(u)=((a+b\alpha)(a+b\alpha+b))/c^2=(a^2+ab+b^2(x+1))/c^2.$$

我们断言 x 不是范数．否则，

$$a^2+ab+b^2(x+1)=c^2x. \tag{2}$$

现在 $a(0)$（即 a 的常数项）或者是 0，或者是 1. 考虑 a 和 b 的常数项的四种情形；即取等式（2）在 $x=0$ 处的值．我们看到 $a(0)=0=b(0)$；即 $x\mid a$ 和 $x\mid b$. 因此，$x^2\mid a^2$ 和 $x^2\mid b^2$，从而等式（2）有 $x^2d=c^2x$ 的形式，其中 $d\in\mathbb{F}_2[x]$．除以 x 得 $xd=c^2$，这迫使 $c(0)=0$；即 $x\mid c$，这是一个矛盾． ■

布饶尔群的进一步讨论见 Cassels-Fröhlich 所编的《Algebraic Number Theory》中 Serre 的论文，Jacobson 所著的《Basic AlgebraII》471～481 页，Reiner 所著的《Maximal Orders》第 5，7，8 章，以及 Kostrikin-Shafarevich 所编的《Encyclopaedia of Mathematical Sciences，AlgebraIX》中 V. P. Platonov 和 V. I. Yanchevskii 的论文 Finite-Dimensional Division Algebras. 特别地，一个**整体域**是一个域，它或者是一个算术数域［即 $\mathbb{Q}$ 的有限扩张］或者是函数域［$k(x)$的有限扩张，其中 k 是有限域］．对每个整体域，我们指定一个*局部域*的族．这些域是用**离散赋值**的方式极好地定义的．域 L 上的一个**离散赋值**是函数 $v:L\to\Gamma\cup\{0\}$，其中 Γ 是乘性无限循环群，使得对一切 a，$b\in L$，

$$v(a)=0 \text{当且仅当 } a=0;$$
$$v(ab)=v(a)v(b);$$
$$v(a+b)=\max\{v(a),v(b)\}.$$

习题 11.15（ⅱ）中有一个离散赋值的等价定义，其中 Γ 是加性无限循环群．现在 $R=\{a\in L:v(a)\leqslant 1\}$ 是整环且 $P=\{a\in L:v(a)<1\}$ 是 R 中的极大理想．我们称 R/P 为 L 关于离散赋值 v 的**剩余域**．一个**局部域**是这样的域，它关于其上的离散赋值形成的度量是完备的，且它的剩余域是有限的．由此，每个局部域或者是 $\mathbb{Q}_p$ 的有限扩张，即 p-进位数（它是 p-进位整数 $\mathbb{Z}_p$ 的分式域），或者同构于 $\mathbb{F}_q[[x]]$，即有限域 $\mathbb{F}_q$ 上的一元形式幂级数环．如果 k 是局部域，则 $\mathrm{Br}(k)\cong H^2(k_s,k^\times)$，其中 k_s/k 是在代数闭域 $\bar{k}$ 中 k 的极大可分扩张．如果 A 是中心单 K-代数，其中 K 是整体域，又如果 K_v 是 K 的局部域，则 $K_v\otimes_K A$ 是中心单 K_v-代数．**哈塞-布饶尔-诺特-阿尔伯特定理**说，如果 A 是整体域 K 上的中心单代数，则 $A\cong K$ 当且仅当对一切相伴局部域 k_v，$K_v\otimes_K A\cong K_v$. 我们仅提及这些被谢瓦莱(C. Chevalley)用来发展*类域论*［它是代数数论的一个分支，涉及有阿贝尔伽罗瓦群的伽罗瓦扩张（可能是无限次的）］的结果．见 Neukirch-Schmidt-Wingberg 所著的《Cohomology of Number Fields》．

关于布饶尔群的推广［例如 $\mathrm{Br}(k)$其中 k 是交换环］以及与森田理论的结合，见 Orzech-Small 所著的《The Brauer Group of Commutative Rings》和 Caenepeel 所著的《Brauer Groups，Hopf Algebras，and Galois Theory》.

习题

10.65　证明叉积(E,G,f)中的结构常数是

$$g_\alpha^{\sigma,\tau}=\begin{cases} f(\sigma,\tau) & \text{如果 } \alpha=\sigma\tau; \\ 0 & \text{其他.}\end{cases}$$

10.66 证明$\mathbb{H}\otimes_{\mathbb{R}}\mathbb{H}\cong \mathrm{Mat}_4(\mathbb{R})$.

10.9 谱序列介绍

我们要提出的最后一个课题是谱序列，它的主要用途是计算同调群和比较复合函子的同调群．简短的本节只描述谱序列的设置，关于更完整的说明读者可参考 Mac Lane 所著的《Homology》第 11 章，McCleary 所著的《User's Guide to Spectral Sequences》，或 Rotman 所著的《An Introduction to Homological Algebra》第 11 章.

称模 K 的一个子模序列

$$K = K_0 \supseteq K_1 \supseteq K_2 \supseteq \cdots \supseteq K_\ell = \{0\}$$

为一个**滤子**（代替正规列），并称商 K_i/K_{i+1}为这个滤子的**因子模**．我们知道模 K 并不被一个滤子的因子模确定；另一方面，因子模的知识确实给出了关于 K 的某些信息．例如，如果一切因子模都是零，则 $K=\{0\}$；如果一切因子模都是有限的，则 K 是有限的（$|K|$ 是因子模的阶之积）；或者如果一切因子模都是有限生成的，则 K 是有限生成的．

定义 如果 K 是模，则 K 的一个**子商**是指同构于 S/T 的一个模，其中 $T\subseteq S\subseteq K$ 是子模．

于是，K 的子商是子模的商．易知 K 的子商也是商的子模（$S/T\subseteq K/T$）．

例 10.134 （i）模 K 的一个滤子的一切因子模都是 K 的子商．

（ii）复形$(\mathbf{C}_\bullet, d_\bullet)$的第 n 个同调群是 C_n 的子商． ■

谱序列在下列意义下计算了同调群 H_n，即它计算了 H_n 的某个滤子的因子模．一般来说，这只给出了关于 H_n 的部分信息，但如果因子模受到很大的约束，则它们可以给出更多的信息，甚至可以完全确定 H_n. 例如，假设 K 的因子模只有一个非零，比如 $K_i/K_{i+1}\cong A\neq\{0\}$；我们断言 $K\cong A$. 这个滤子的起首是

$$K = K_0 \supseteq K_1 \supseteq \cdots \supseteq K_i.$$

因 $K_0/K_1=\{0\}$，有 $K=K_0=K_1$. 类似地，$K_1/K_2=\{0\}$给出 $K_1=K_2$；事实上，$K=K_0=K_1=\cdots=K_i$. 类似的论证，计算了滤子的结尾．例如，因$K_{\ell-1}/K_\ell=\{0\}$,有$K_{\ell-1}=K_\ell=\{0\}$；于是，滤子是

$$K = K_0 = \cdots = K_i \supsetneq K_{i+1} = \cdots = K_\ell = \{0\},$$

因此 $K\cong K/\{0\} = K_i/K_{i+1}\cong A$.

为了理解谱序列，我们必须认识一个显然的事实：如果能够提出额外的简化假设，则非常一般的陈述就可以变得很有用．

谱序列常在下列背景中产生．一个**双重分次模** $M=M_{\bullet\bullet}$是指模 $M_{p,q}$的一个双指标族，其中 p，$q\in\mathbb{Z}$；我们画出双重分次模为模的一个集合，一个位于平面中每个格点(p,q)上．于是，举例来说，有**第一象限**双重分次模，当 p 或 q 为负数时有 $M_{p,q}=\{0\}$；类似地，有**第三象限**双重分次模．**二重复形**是指一个双重分次模，它有垂直箭头 $d''_{p,q}: M_{p,q}\to M_{p,q-1}$ 构成列复形，还有水平箭头 $d'_{p,q}: M_{p,q}\to M_{p-1,q}$ 构成行复形，且它的方块反交换：

$$\begin{array}{ccc} M_{p-1,q} & \xleftarrow{d'_{p,q}} & M_{p,q} \\ \downarrow{\scriptstyle d''_{p-1,q}} & & \downarrow{\scriptstyle d''_{p,q}} \\ M_{p-1,q-1} & \xleftarrow[d'_{p,q-1}]{} & M_{p,q-1} \end{array}$$

即 $d'd''+d''d'=0$. 反交换的理由是允许我们定义二重复形 M 的**全复形** Tot（M）：它的 n 次项是

$$\mathrm{Tot}(M)_n = \sum_{p+q=n} M_{p,q};$$

它的微分 $d_n: \mathrm{Tot}(M)_n \to \mathrm{Tot}(M)_{n-1}$ 由

$$d_n = \sum_{p+q=n} d'_{p,q} + d''_{p,q}$$

给出．反交换迫使 $d_{n-1}d_n = 0$:

$$dd = (d'+d'')(d'+d'') = d'd' + (d'd'' + d''d') + d''d'' = 0;$$

于是，$\mathrm{Tot}(M)$是复形．

一切双重分次模形成一个范畴．给定整数的有序对(a,b)，一个映射族$f_{p,q}: M_{p,q} \to L_{p+a,q+b}$叫做$(a,b)$**双次映射** $f: M_{..} \to L_{...}$ 例如，上面的映射 d'和 d''分别有双次数$(0,-1)$和$(-1,0)$．容易验证一切双重分次模和一切双次映射形成一个范畴．复合的一个好的特性是双次数相加：如果 f 的双次数为(a,b)而 f'的双次数为(a',b')，则它们的复合 $f'f$ 的双次数为$(a+a',b+b')$．双重分次模的映射用来建立某种正合列．例如，五项正合列的一个证明用到这些映射．

谱序列是指二重复形 $E^r_{p,q}$对一切 $r \geq 2$ 的一个序列，其中每个 $E^{r+1}_{p,q}$是 $E^r_{p,q}$的子商（我们还必须指定从那些 $E^r_{p,q}$形成的二重复形 $E^{r+1}_{p,q}$的同态）．大多数谱序列由 $\mathrm{Tot}(M)$的滤子形成，其中 $M_{..}$是二重复形．特别地，有两个"常用"的滤子（如果 $M_{..}$是第一象限的或第三象限的)，它们确定的谱序列记为 ${}^{\mathrm{I}}E^r_{p,q}$和 ${}^{\mathrm{II}}E^r_{p,q}$.

我们说谱序列 $E^r_{p,q}$**收敛**到（单分次的）模 H．（记为 $E^2_{p,q} \Rightarrow H_n$），如果每个 H_n 有因子模为

$$E_{0,n}, E_{1,n-1}, \cdots, E_{n,0}$$

的滤子，且对一切满足 $p+q=n$ 的 p，q，因子模 $E_{p,q}$是 $E^2_{p,q}$的子商．在运用谱序列之前有两个步骤要确立．

定理Ⅰ　*如果 $M_{..}$是第一象限或第三象限的二重复形，则*

$${}^{\mathrm{I}}E^2_{p,q} \Rightarrow H_n(\mathrm{Tot}(M)) \text{ 和 } {}^{\mathrm{II}}E^2_{p,q} \Rightarrow H_n(\mathrm{Tot}(M)).$$

于是，对每个 n，存在 $\mathrm{Tot}(M)_n$ 的两个滤子；一个的因子模是 ${}^{\mathrm{I}}E^2_{p,q}$的子商，另一个的因子模是 ${}^{\mathrm{II}}E^2_{p,q}$的子商（和通常一样，在这个上下文中，$p+q=n$)，且两者收敛到同一目标．

定理Ⅱ　*如果 $M_{..}$是第一象限或第三象限的二重复形，则对每个 p，q，存在关于 ${}^{\mathrm{I}}E^2_{p,q}$和 ${}^{\mathrm{II}}E^2_{p,q}$的公式．*

定理Ⅱ提供了计算 $E^2_{p,q}$的子商的可能性．

我们概要证明 $\mathrm{Tor}_n(A,B)$不依赖于被分解的变量，以此说明定义为 $H_n(\mathbf{P}_A \otimes B)$的 $\mathrm{Tor}_n(A,B)$的值（其中 $\mathbf{P}_A$ 是 A 的删除投射分解）和定义为 H_n（$A \otimes \mathbf{Q}_B$)（其中 $\mathbf{Q}_B$ 是 B 的删除投射分解）的 $\mathrm{Tor}_n(A,B)$是一致的．证明的思想是用两个变量的分解同时分解它们．定义第一象限双重分次模 $M = \mathbf{P}_A \otimes \mathbf{Q}_B$，它的 p，q 项是 $P_p \otimes Q_q$；定义垂直箭头 $d''_{p,q} = (-1)^p 1 \otimes \partial_q: P_p \otimes Q_q \to P_p \otimes Q_{q-1}$和水平箭头 $d'_{p,q} = \Delta_p \otimes 1: P_p \otimes Q_q \to P_{p-1} \otimes Q_q$，其中 ∂_n是 $\mathbf{Q}_B$ 中的微分而 Δ_n 是 $\mathbf{P}_A$ 中的微分（符号迫使反交换），从而组成一个双复形．公式的存在性是定理Ⅱ所陈述的，因为此时第一个谱序列${}^{\mathrm{I}}E^2_{p,q}$给出

$${}^{\mathrm{I}}E^2_{p,q} = \begin{cases} \{0\} & \text{如果 } q > 0; \\ H_q(\mathbf{P}_A \otimes B) & \text{如果 } q = 0. \end{cases}$$

因 $\{0\}$ 的子商必是 $\{0\}$，因此 $H_n(\mathrm{Tot}(M))$ 的滤子的因子模除了一个之外都是零，从而

$$H_n(\mathrm{Tot}(M)) \cong H_n(\mathbf{P}_A \otimes B).$$

类似地，定理Ⅱ中提到的公式对第二个谱序列给出

$$^{\mathrm{II}}E^2_{p,q}=\begin{cases}\{0\} & \text{如果 } p>0;\\ H_q(A\otimes \mathbf{Q}_B) & \text{如果 } p=0.\end{cases}$$

同样，$H_n(\mathrm{Tot}(M))$的滤子只有一个可能非零的因子模，从而

$$H_n(\mathrm{Tot}(M))\cong H_n(A\otimes \mathbf{Q}_B).$$

所以，

$$H_n(\mathbf{P}_A\otimes B)\cong H_n(\mathrm{Tot}(M))\cong H_n(\mathbf{P}_A\otimes B).$$

我们已经证明了 Tor 不依赖于被分解的变量．

下面是一个上同调的结果，它说明谱序列如何用来计算复合函子．把提升指标的约定延伸到这里，记第三象限二重复形中的模 $M_{-p,-q}$ 为 $M^{p,q}$．

定理 10.135（格罗滕迪克） *设 $F:\mathcal{B}\to\mathcal{C}$ 和 $G:\mathcal{A}\to\mathcal{B}$ 是加性函子，其中 $\mathcal{A}$，$\mathcal{B}$ 和 $\mathcal{C}$ 是模范畴．如果 F 是左正合的而 E 是 $\mathcal{A}$ 中的内射模蕴涵对一切 $m>0$，$(R^mF)(GE)=\{0\}$（其中 R^mF 是 F 的右导函子），则对每个模 $A\in\mathcal{A}$，存在第三象限谱序列*

$$E_2^{p,q}=(R^pF)(R^qG(A))\Rightarrow R^n(FG)(A).$$

证明见 Rotman 所著的《An Introduction to Homological Algebra》，350 页．

下一结果证明，如果 N 是群 Π 的正规子群，则 N 的上同调群和 Π/N 的上同调群能够用来计算 Π 的上同调群．

定理 10.136（林登-霍赫希尔德-塞尔） *设 Π 是群，它有正规子群 N．对每个 Π-模 A，存在第三象限谱序列使得*

$$E_2^{p,q}=H^p(\Pi/N,H^q(N,A))\Rightarrow H^n(\Pi,A).$$

证明 定义函子 $G:{}_{\mathbb{Z}\Pi}\mathbf{Mod}\to{}_{\mathbb{Z}(\Pi/N)}\mathbf{Mod}$ 和 $F:{}_{\mathbb{Z}(\Pi/N)}\mathbf{Mod}\to\mathbf{Ab}$ 为 $G=\mathrm{Hom}_N(\mathbb{Z},\ )$ 和 $F=\mathrm{Hom}_{\Pi/N}(\mathbb{Z},\ )$. 当然，$F$ 是左正合的，且易知 $FG=\mathrm{Hom}_\Pi(\mathbb{Z},\ )$．只要 E 是内射 Π-模和 $m>0$ 时就有 $H^m(\Pi/N,E)=\{0\}$ 的证明可在 Rotman 所著的《An Introduction to Homological Algebra》307 页找到．现在结果由定理 10.135 得到． ■

1948 年林登（Lyndon）在他的学位论文中为了计算有限生成阿贝尔群 Π 的上同调群而发现了这个定理．几年之后，霍赫希尔德（Hochschild）和塞尔（Serre）把这个结果表达为现在的形式．

第11章 交换环Ⅲ

11.1 局部和整体

通常在考察代数结构时“一次考察一个素数”比较容易．设G和H是有限群．如果$G\cong H$，则对一切素数p，它们的西罗p-子群同构；*局部地*研究G和H的意思是研究它们的p-子群．这种局部信息并不足以确定是否$G\cong H$；例如，S_3和$\mathbb{I}_6$是不同构的群，但有同构的西罗子群．整体问题假定对一切素数p，群G和H的西罗p-子群同构，问推出$G\cong H$还有什么是必需的．在群的情形中，这导致扩张问题和群的上同调（但要解决整体问题这还是不充分的：例如，S_3和$\mathbb{I}_6$有同构的西罗子群和相同的合成因子）．这种技术的一个成功的描述是由有限阿贝尔群提供的．局部问题涉及准素分量（西罗子群），它是循环群的直和，而整体问题由准素分解得以解决：每个有限阿贝尔群是它的准素分量的直和．此时，局部信息对解整体问题是充分的．局部/整体方法的好处是局部问题比整体问题简单且它的解是有价值的．本节我们先从局部和整体研究的另一种群论说明开始，然后考虑交换环的局部化．

定义 *设R是整环且$Q=\mathrm{Frac}(R)$．如果M是R-模，定义*

$$\mathrm{rank}(M)=\dim_Q(Q\otimes_R M).$$

例如，一个阿贝尔群G的秩定义为$\dim_{\mathbb{Q}}(\mathbb{Q}\otimes_{\mathbb{Z}}G)$．

回忆如果R是整环，则一个R-模是*无挠的*如果它没有有限阶非零元素；即如果$r\in R$和$m\in M$都是非零的，则rm是非零的．

引理 11.1 *设R是整环，且$Q=\mathrm{Frac}(R)$，并设M是无挠R-模．则M的秩为1当且仅当它同构于Q的一个非零R-子模．*

证明 如果$\mathrm{rank}(M)=1$，则$M\neq\{0\}$．$0\to R\to Q$的正合性给出

$$\mathrm{Tor}_1^R(Q/R,M)\to R\otimes_R M\to Q\otimes_R M$$

的正合性．根据引理10.101(ⅲ)，有$\mathrm{Tor}_1^R(Q/R,M)\cong tM$，它是$M$的挠子模，从而$\mathrm{Tor}_1^R(Q/R,M)=\{0\}$，这是因为$M$是无挠的．但命题8.86给出$R\otimes_R M\cong M$，而$M$的秩为1，因此$Q\otimes_R M\cong Q$．所以，$M$同构于$Q$的一个$R$-子模．

反之，如果M同构于Q的一个R-子模，则存在正合列$0\to M\to Q$．因Q是平坦R-模，根据系8.103，有$0\to Q\otimes_R M\to Q\otimes_R Q$的正合性．这是$Q$上向量空间的正合列，且$Q\otimes_R Q\cong Q$的维数为1．所以，非零子空间$Q\otimes_R M$的维数也是1；即$\mathrm{rank}(M)=1$． ■

例 11.2 下面的阿贝尔群是无挠的，且秩为1：

(ⅰ) 整数群$\mathbb{Z}$；

(ⅱ) 加法群$\mathbb{Q}$；

(ⅲ) 有有限十进制展开式的一切有理数的集合；

(ⅳ) 分母无平方因数的一切有理数的集合． ■

命题 11.3 *设R是整环，且$Q=\mathrm{Frac}(R)$．Q的两个子模A和B同构当且仅当存在$c\in Q$使得*

$B = cA$.

证明 如果 $B = cA$，则经 $a \mapsto ca$ 有 $A \cong B$.

反之，假设 $f: A \to B$ 是同构. 我们先证明如果 $a \in A$ 非零，则 f 由它在 $\langle a \rangle$ 上的值确定：如果 $g: A \to B$ 和 $g/\langle a \rangle = f \mid \langle a \rangle$，则 $f = g$. 如果 $x \in A$，则存在 $r, s \in R$ 使得 $sx = ra \in \langle a \rangle$（因为 A 是 Q 的子模），从而

$$f(sx) = f(ra) = rf(a) = rg(a) = g(ra) = g(sx).$$

因此，$s(f(x) - g(x)) = 0$，又因 B 是无挠的，有 $f(x) = g(x)$.

如果 $f(a) = b$，定义 $c = b/a$. 为证明对一切 $x \in A$ 有 $f(x) = cx$，现在只需证明对一切 $r \in R$，$f(ra) = c(ra)$. 但

$$f(ra) = rf(a) = rb = r(b/a)a = c(ra).$$

由此对一切 $x \in A$，$f(x) = cx$，从而 $B = cA$. ■

定义 对每个素数 p，定义$\mathbb{Q}$的一个子环，

$$\mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q} : (b, p) = 1\}.$$

命题 11.4 （i）对每个素数 p，环$\mathbb{Z}_{(p)}$是一个局部[⊖]PID.

（ii）如果 G 是秩为 1 的无挠阿贝尔群，则$\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} G$ 是秩为 1 的无挠$\mathbb{Z}_{(p)}$-模.

（iii）如果 M 是秩为 1 的无挠 $\mathbb{Z}_{(p)}$-模，则 $M \cong \mathbb{Z}_{(p)}$ 或 $M \cong \mathbb{Q}$.

证明 (i) 我们证明 $\mathbb{Z}_{(p)}$ 中仅有的非零理想 I 是 (p^n)，其中 $n \geqslant 0$；由此可知 $\mathbb{Z}_{(p)}$ 是 PID，且 (p) 是它唯一的极大理想. 因 $\mathbb{Z}_{(p)} \subseteq \mathbb{Q}$，每个非零 $x \in p^{-1}\mathbb{Z}$ 有 a/b 的形式，其中 a 和 b 是整数且 $(b, p) = 1$. 但 $a = p^n a'$，其中 $n \geqslant 0$ 且 $(a', p) = 1$；即存在单位 $u \in \mathbb{Z}_{(p)}$，就是$u = a'/b$，使得 $x = up^n$. 设 $I \neq \{0\}$ 是理想. 在 I 的一切非零元素之中，选取 $x = up^n \in I$，其中 u 是单位且 n 极小. 如果 $y \in I$，则 $y = vp^m$，其中 v 是单位且 $n \leqslant m$，从而 $I = (x) = (p^n)$. 因此，$p^n \mid y$ 且 $y \in (p^n)$.

（ii）因 $\mathbb{Z}_{(p)} \subseteq \mathbb{Q}$，它是一个秩为 1 的加法无挠阿贝尔群，从而它是平坦的（系 9.6）. 因此，$0 \to G \to \mathbb{Q}$ 的正合性给出

$$0 \to \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} G \to \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} \mathbb{Q}$$

的正合性. 根据习题 11.5，$\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q} = \mathrm{Frac}(\mathbb{Z}_{(p)})$，因此 $\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} G$ 是秩为 1 的无挠 $\mathbb{Z}_{(p)}$-模.

(iii) 不失一般性，可假定 $M \subseteq \mathbb{Q}$ 和 $1 \in M$. 考虑方程 $p^n y_n = 1, n \geqslant 0$. 我们断言，如果所有这些方程对 $y_n \in M$ 有解，则 $M = \mathbb{Q}$. 如果 $a/b \in \mathbb{Q}$，则 $a/b = a/p^n b'$，其中 $(b', p) = 1$，从而 $a/b = (a/b')y_n$；因 $a/b' \in \mathbb{Z}_{(p)}$，有 $a/b \in M$. 现在可以假定存在最大的 $n \geqslant 0$ 使得方程 $p^n y_n = 1$ 对 $y_n \in M$ 有解. 我们断言 $M = \langle y_n \rangle$，它是由 y_n 生成的循环子模，这就证明了 $M \cong \mathbb{Z}_{(p)}$. 如果 $m \in M$，则 $m = c/d = p^r c'/p^s d' = (c'/d')/(1/p^{s-r})$，其中 $(c', p) = 1 = (d', p)$. 因 c'/d' 是 $\mathbb{Z}_{(p)}$ 中的单位，有 $1/p^{s-r} \in M$，从而 $s - r \leqslant n$；即有某个 $\ell \geqslant 0$ 使得 $s - r = n - \ell$. 因此，$1/p^{s-r} = 1/p^{n-\ell} = p^\ell/p^n = p^\ell y_n$，从而 $m = (c'p^\ell/d')y_n \in \langle y_n \rangle$. ■

定义 **离散赋值环**是指一个不是域的局部 PID，缩写为 DVR.

例如，$\mathbb{Z}_{(p)}$ 是 DVR.

定义 如果两个秩为 1 的无挠阿贝尔群 G 和 H 对一切素数 p 有 $\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} G \cong \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} H$，则称

⊖ 回忆局部环是有唯一极大理想的交换环. 多数作者强调局部环是诺特环［$\mathbb{Z}_{(p)}$ 甚至是 PID］. 有些作者允许局部环是非交换的，把局部环定义为有唯一极大左理想 $\mathfrak{m}$ 的环. 此时 $\mathfrak{m} = J(R)$，雅各布森根，从而它是一个双边理想.

G 和 H 是**局部同构的**.

对秩为 1 的无挠阿贝尔群 G，我们已经解决了局部问题，即把 G 和 $\mathbb{Z}_{(p)}$-模的族 $\mathbb{Z}_{(p)}\otimes_{\mathbb{Z}}G$ 联系起来，其中对每个素数 p 有一个 $\mathbb{Z}_{(p)}\otimes_{\mathbb{Z}}G$.

例 11.5 设 G 是分母无平方因数的那些有理数组成的 $\mathbb{Q}$ 的子群，则 G 和 $\mathbb{Z}$ 是局部同构的，但它们不同构，因为 G 不是有限生成的. ■

我们现在对秩为 1 的无挠阿贝尔群考虑整体问题.

定义 设 G 是阿贝尔群. 对 $x\in G$ 和素数 p，如果存在 $y_n\in G$ 使得 $p^n y_n=x$，我们说 x **在 G 中被 p^n 整除**. 定义 x 的 **p-高度**（记为 $h_p(x)$）为

$$h_p(x)=\begin{cases}\infty & \text{如果对一切 } n\geqslant 0, x \text{ 在 } G \text{ 中被 } p^n \text{ 整除}\\ k & \text{如果 } x \text{ 在 } G \text{ 中被 } p^k \text{ 整除但不被 } p^{k+1} \text{ 整除}.\end{cases}$$

x 在 G 中的**高度序列**（或**特征**）（其中 x 非零）是指序列

$$\chi(x)=\chi_G(x)=(h_2(x),h_3(x),h_5(x),\cdots,h_p(x),\cdots).$$

于是，$\chi(x)$ 是序列 (h_p)，其中 $h_p=\infty$ 或 $h_p\in\mathbb{N}$. 设 $G\subseteq\mathbb{Q}$，并设 $x\in G$ 是非零元素. 如果 $\chi(x)=(h_p)$ 和 $a=p_1^{f_1}\cdots p_n^{f_n}$，则 $\frac{1}{a}x\in G$ 当且仅当对 $i=1,\cdots,n$ 有 $f_{p_i}\leqslant h_{p_i}$.

例 11.6 例 11.2 中的每个群都包含 $x=1$.

（i）在 $\mathbb{Z}$ 中，

$$\chi_{\mathbb{Z}}(1)=(0,0,0,\cdots).$$

（ii）在 $\mathbb{Q}$ 中，

$$\chi_{\mathbb{Q}}(1)=(\infty,\infty,\infty,\cdots).$$

（iii）如果 G 是有有限十进制展开式的一切有理数的群，则

$$\chi_G(1)=(\infty,0,\infty,0,0,\cdots).$$

（iv）如果 H 是分母无平方因数的有理数的群，则

$$\chi_H(1)=(1,1,1,\cdots).$$ ■

秩为 1 的无挠阿贝尔群中不同元素可以有不同的高度序列. 例如，如果 G 是有有限十进制展开式的有理数的群，则 1 和 $\frac{63}{8}$ 在 G 中，且

$$\chi(1)=(\infty,0,\infty,\cdots),\chi\left(\frac{63}{8}\right)=(\infty,2,\infty,1,0,0,\cdots).$$

于是，这两个高度序列对无限 p-高度是一致的，但对两个有限 p-高度是不一致的.

定义 如果两个高度序列 $(h_2,h_3,\cdots,h_p,\cdots)$ 和 $(k_2,k_3,\cdots,k_p,\cdots)$ 中只有有限个 p 使得 $h_p\neq k_p$，且对这样的素数 p，h_p 和 k_p 都不是 ∞，则称这两个高度序列**等价**，记为

$$(h_2,h_3,\cdots,h_p,\cdots)\sim(k_2,k_3,\cdots,k_p,\cdots).$$

易知这个等价事实上是一个等价关系.

引理 11.7 如果 G 是秩为 1 的无挠阿贝尔群，又如果 $x,y\in G$ 是非零元素，则它们的高度序列 $\chi(x)$ 和 $\chi(y)$ 等价.

证明 可以假定 $G\subseteq\mathbb{Q}$. 如果 $b=p_1^{e_1}\cdots p_n^{e_n}$，则易知对一切 $p\notin\{p_1,\cdots,p_n\}$，$h_p(bx)=h_p(x)$，而对 $i=1,\cdots,n$，

$$h_{p_i}(bx) = e_i + h_{p_i}(x)$$

(我们约定 $e_i+\infty=\infty$). 因此，$\chi(x)\sim\chi(bx)$. 因 $x,y\in G\subseteq \mathbb{Q}$，有整数 a，b 使得 $x/y=a/b$，从而 $bx=ay$. 所以，$\chi(x)\sim\chi(bx)=\chi(ay)\sim\chi(y)$. ■

定义 高度序列的等价类叫做型. 如果 G 是秩为 1 的无挠阿贝尔群，则它的型是高度序列 $\chi(x)$ 的型，记为 $\tau(G)$，其中 x 是 G 的一个非零元素.

引理 11.7 证明 $\tau(G)$ 只依赖于 G 而不依赖于非零元素 $x\in G$ 的选取. 我们现在解整体问题.

定理 11.8 如果 G 和 H 都是秩为 1 的无挠阿贝尔群，则 $G\cong H$ 当且仅当 $\tau(G)=\tau(H)$.

证明 设 $\varphi: G\to H$ 是同构. 如果 $x\in G$ 非零，易知 $\chi(x)=\chi(\varphi(x))$，从而 $\tau(G)=\tau(H)$.

关于逆命题，不失一般性可假定 G 和 H 都是 $\mathbb{Q}$ 的子群. 选取非零 $x\in G$ 和 $y\in H$. 根据等价的定义，存在素数 $p_1,\cdots,p_n,q_1,\cdots,q_m$ 使得 $h_{p_i}(x)<h_{p_i}(y)<\infty$，$\infty>h_{q_j}(x)>h_{q_j}(y)$，且对其他一切素数 p，$h_p(x)=h_p(y)$. 定义 $b=\prod p_i^{h_{p_i}(y)-h_{p_i}(x)}$，则 $bx\in G$ 和 $h_{p_i}(bx)=(h_{p_i}(y)-h_{p_i}(x))+h_{p_i}(x)=h_{p_i}(y)$. 用 $a=\prod q_i^{h_{q_i}(x)-h_{q_i}(y)}$ 的类似构造可得 $\chi(bx)=\chi(ay)$. 我们已经找到元素 $x'=bx\in G$ 和 $y'=ay\in H$ 有相同的高度序列.

定义 $\varphi: G\to\mathbb{Q}$ 为 $\varphi(g)=\frac{y'}{x'}g$. 显然 φ 是一个单同态. 我们断言 $\mathrm{im}\varphi\subseteq H$. 因每个 $g\in G$ 能够写作 $g=\frac{1}{c}x'$，只需证明如果 $\frac{1}{c}x'\in G$，则 $\varphi(\frac{1}{c}x')=\frac{1}{c}y'\in H$. 但如果 $c=p_1^{f_1}\cdots p_t^{f_t}$，则 $\frac{1}{c}x'\in G$ 当且仅当 $f_p\leqslant h_p(x')$. 因 $\chi(x')=\chi(y')$，$\frac{1}{c}y'\in H$ 当且仅当 $f_p\leqslant h_p(y')=h_p(x')$. 于是，可以把 φ 看作映射 $G\to H$. 最后，为证明 φ 是满射，注意它的逆由 $H\to G$ 的映射 $h\mapsto\frac{x'}{y'}h$ 给出. ■

刚才证明的唯一性定理由一个存在性定理补足.

命题 11.9 给定高度序列 $(k_2,k_3,\cdots,k_p,\cdots)$，其中 $0\leqslant k_p\leqslant\infty$，存在唯一的包含 1 的子群 $G\subseteq\mathbb{Q}$ 使得对一切 p 有 $h_p(1)=k_p$. 于是，给定任意型 τ，存在秩为 1 的无挠阿贝尔群 G 使得 $\tau(G)=\tau$，且不计同构是唯一的.

证明 定义

$$D=\{a\in\mathbb{Z}: a=\prod p_i^{e_i}\text{，其中对一切 } i, 0\leqslant e_i\leqslant k_{p_i}\}$$

(如果 $k_{p_i}=\infty$，则 $0\leqslant e_i\leqslant k_{p_i}$ 的意思是 $e_i\in\mathbb{N}$)，并定义

$$G=\{m/a\in\mathbb{Q}: m\in\mathbb{Z}\text{ 和 } a\in D\}.$$

为证明 G 是 $\mathbb{Q}$ 的子群，只需证明它在加法下封闭. 设 m/a 和 n/b 和都在 G 中，其中 $a=\prod p_i^{e_i}$，$b=\prod p_i^{f_i}$，且 $\max\{e_i,f_i\}\leqslant k_{p_i}$；即 $[a,b]\in D$. 现在

$$\frac{m}{a}+\frac{n}{b}=\frac{ma'+nb'}{[a,b]},$$

其中 $[a,b]=\mathrm{lcm}\{a,b\}=\prod p_i^{\max\{e_i,f_i\}}$，$a'=[a,b]/a$，$b'=[a,b]/b$. 因 $[a,b]\in D$，有 $m/a+n/b\in G$. 显然对一切 p，$h_p(1)=k_p$，因此 $\tau(G)=\tau$.

现在证明唯一性. 设 G 和 H 都是包含 1 的 $\mathbb{Q}$ 的子群满足 $\chi_H(1)=\chi_G(1)$. 假设 $m/d\in H$ 是既约的，即 $(m,d)=1$. 则存在整数 s 和 t 使得 $1=sm+td$，从而 $1/d=s(m/d)+td/d\in H$. 另一方面，根据高度序列的定义，$1/d\in G$. 因为 H 是由形如 $1/d$ 的一切元素生成的，所以 $H\subseteq G$. 可类似地证

明反包含，因此 $G=H$. ■

系 11.10 （i）存在 $\mathbb{Q}$ 的不可数个不同构的子群.

（ii）如果 R 是 $\mathbb{Q}$ 的子环，则 1 的高度序列由 0 和∞组成.

（iii）存在不可数个不同构的 $\mathbb{Q}$ 的子环. 事实上，$\mathbb{Q}$ 的不同子环作为环都是不同构的.

证明 （i）给定型 τ，命题 11.9 提供秩为 1 的无挠阿贝尔群 G 满足 $\tau(G)=\tau$. 但型有不可数个；例如，由 0 和∞组成的两个高度序列等价当且仅当它们相等.

（ii）如果 $h_p(1)>0$，则 $\frac{1}{p}\in R$. 因 R 是环，对一切 $n\geqslant 1$，$\left(\frac{1}{p}\right)^n=\frac{1}{p^n}\in R$，从而 $h_p(1)=\infty$.

（iii）如果 R 和 S 是 $\mathbb{Q}$ 的不同子群，则根据（ii），1 的高度序列是不同的. 两个陈述都来自下列结论：仅由 0 和∞组成的高度序列等价当且仅当它们相等. ■

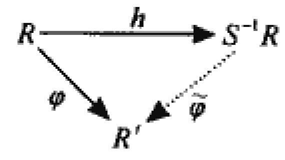
A. G. Kurosh 对有有限秩 n 的无挠阿贝尔群 G 进行了分类，他使用了不变量 $n=\mathrm{rank}(G)$，关于一切素数 p 的 $\dim(\mathbb{F}_p\otimes G)$ 以及序列 (M_p) 的一个等价类，其中 M_p 是 p-进位数 $\mathbb{Q}_p$ 上的非奇异 $n\times n$ 矩阵（这个定理不容易应用，因为几乎不可能确定两个群是否有等价的矩阵序列）. 易知每个这样的群 G 是不可分解[⊖]群的直和；然而，这样的分解事实上没有唯一性. 例如，存在群 G 满足

$$G=A_1\oplus A_2=B_1\oplus B_2\oplus B_3,$$

其中一切直和项不可分解，$\mathrm{rank}(A_1)=1$，$\mathrm{rank}(A_2)=5$，且对 $j=1,2,3,\mathrm{rank}(B_j)=2$. 于是，在一个分解中，不可分解直和项的个数不是由 G 唯一确定的，任何不可分解直和项的同构类的个数也不能确定. 这里有一个 A. L. S. Corner 的有趣定理（它可以用来产生诸如刚才讨论的群 G 那样的无挠群的坏例）. 设 R 是环，它的加法群是可数的、无挠的和约化的（没有非零可除子群），则存在阿贝尔群 G，它也是可数的、无挠的、约化的，使得 $\mathrm{End}(G)\cong R$. 此外，如果 R 的加法群有有限秩 n，则可选取 G 使它有秩 $2n$. 证明见 Fuchs 所著的《Infinite Abelian Groups II》，231 页.

交换环的局部方法推广了从 $\mathbb{Z}$ 到局部环 $\mathbb{Z}_{(p)}$ 的构造. 给定交换环 R 的一个乘法下封闭的子集 S，多数作者把整环 R 的分式域的（乏味的）构造方法加以推广，以此构造局部化 $S^{-1}R$. 他们定义 $R\times S$ 上的一个关系为 $(r,\sigma)\equiv(r',\sigma')$，如果存在 $\sigma''\in S$ 使得 $\sigma''(r\sigma'-r'\sigma)=0$（当 R 是整环而 S 是一切非零元素的子集时，这个定义简化为涉及交叉乘法的通常定义）. 在证明了这是一个等价关系之后，$S^{-1}R$ 被定义为一切等价类的集合，再定义加法和乘法并证明是合理定义的，然后验证 R-代数的一切公理，并证明 S 的元素是可逆的. 换句话说，把 $S^{-1}R$ 的元素看作分母在 S 中的分数. 我们偏爱用另一种方式来建立 $S^{-1}R$ 的存在性和初等性质，它较不乏味，还可展示如何产生等价关系对交叉乘法的推广.

定义 设 R 是交换环并设 S 是 R 的任一子集. R 的一个**局部化**是指一个 R-代数 $S^{-1}R$ 和一个称为**局部化映射**的 R-代数映射 $h:R\to S^{-1}R$，满足对每个 $s\in S$，$h(s)$ 在 $S^{-1}R$ 中可逆，且 $S^{-1}R$ 是下面的泛映射问题的解.



如果 R' 是交换 R-代数和 $\varphi:R\to R'$ 是 R-代数映射满足对一切 $s\in S$，$\varphi(s)$ 在 R' 中可逆，则存在唯一

⊖ 一个阿贝尔群 G 是不可分解的，如果不存在非零群 A 和 B 满足 $G\cong A\oplus B$.

的 R-代数映射 $\tilde{\varphi}: S^{-1}R \to R'$ 使得 $\tilde{\varphi}h = \varphi$.

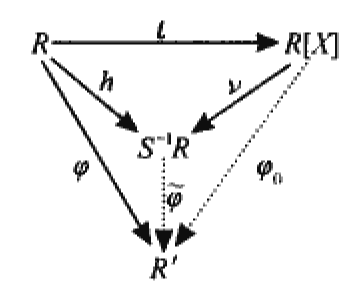
局部化 $S^{-1}R$ 如果存在，则和任意泛映射问题的解一样，如不计同构是唯一的.

定理 11.11 对交换环 R 的每个子集 S，存在局部化 $S^{-1}R$.

证明 设 $X = \{x_s : s \in S\}$ 是使得 $x_s \mapsto s$ 构成双射 $X \to S$ 的集合，并设 $R[X]$ 是 R 上变量为 X 的多项式环. 定义

$$S^{-1}R = R[X]/I,$$

其中 I 是由 $\{sx_s - 1 : s \in S\}$ 生成的理想，并定义 $h: R \to S^{-1}R$ 为 $h: r \mapsto r + I$，其中 r 是常数多项式. 显然 $S^{-1}R$ 是 R-代数，h 是 R-代数映射，且每个 $h(s)$ 可逆. 现在假定 R' 是一个 R-代数，$\varphi: R \to R'$ 是 R-代数映射，且对一切 $s \in S$，$\varphi(s)$ 可逆. 考虑下面的图，其中顶上的箭头 $\iota: R \to R[X]$ 把每个 $r \in R$ 送到常数多项式 r，$\nu: R[X] \to S^{-1}R$ 是自然映射.



因为 h 和 $\nu\iota$ 都把 $r \in R$ 送到 $r+1$，所以最上面的一个三角形交换. 因 $R[X]$ 是 X 上的自由交换 R-代数，存在 R-代数映射 $\varphi_0: R[X] \to R'$ 使得对一切 $s \in S$，$\varphi_0(x_s) = \varphi(s)^{-1}$. 显然，因 $\varphi_0(sx_s - 1) = 0$，从而 $I \subseteq \ker\varphi_0$，由此存在 R-代数映射 $\tilde{\varphi}: S^{-1}R = R[X]/I \to R'$ 使得图交换. 由于 $S^{-1}R$ 作为 R-代数是由 $\mathrm{im}h \cup \{h(s)^{-1} : s \in S\}$ 生成的，因此 $\tilde{\varphi}$ 是唯一的这种映射. ■

下一定义在这个背景下是自然的，因为如果 s, s' 是某个交换环中的可逆元素，则它们的积 ss' 也是可逆的.

定义 如果交换环 R 的一个子集 S 满足 $1 \in S$ 且 $s, s' \in S$ 蕴涵 $ss' \in S$，则称 S 是**乘法封闭的**. 每个交换环是一个乘法幺半群. 如果 S 是 R 的任一子集（可能为空），则

$$\overline{S} = S \text{ 生成的 } R \text{ 的子幺半群}.$$

我们称 $\overline{S}$ 为 S **生成的乘法封闭子集**.

习题 11.8 说 $(\overline{S})^{-1}R \cong S^{-1}R$.

例 11.12 （i）如果 R 是交换环和 $s \in R$，则 $\overline{\{s\}} = \{1, s, s^2, s^3, \cdots\}$ 是元素 s 生成的乘法封闭集.

（ii）如果 $\mathfrak{p}$ 是 R 中的素理想，则 $a \notin \mathfrak{p}$ 和 $b \notin \mathfrak{p}$ 蕴涵 $ab \notin \mathfrak{p}$. 换句话说，补 $R - \mathfrak{p}$ 是乘法封闭的.

（iii）设 P 是 $\mathbb{Z}$ 中一切素数的集合. 如果 $S \subseteq P$，则

$$\overline{S} = \{p_1^{e_1} \cdots p_n^{e_n} : p_i \in S \text{ 和 } e_i \geqslant 0\}. \quad ■$$

我们现在描述 $S^{-1}R$ 中的元素.

命题 11.13 如果 S 是交换环 R 的子集，则每个 $y \in S^{-1}R$ 有一个（未必唯一）因子分解

$$y = h(r)h(\sigma)^{-1}, \text{其中 } r \in R \text{ 和 } \sigma \in \overline{S}.$$

证明 存在性定理把 $S^{-1}R$ 构造为 $R[X]/I$，其中 $X = \{x_s : s \in S\}$ 和 $I = \{sx_s - 1 : s \in S\}$. 于是，每个 $y \in S^{-1}R$ 形如 $y = f(x_1, \cdots, x_n) + I$，其中对某个 $s_i \in S$，$x_i = x_{s_i}$. 对 $n \geqslant 0$ 用归纳法证明该命题. 如果 $n = 0$，则 $f \in R$ 和 $y = h(f)$. 关于归纳步，设 $y = f(x_1, \cdots, x_n) + I$. 记 $(x_1, \cdots, x_{n-1}) = X, x_n = x$，且

$$f(X,x_n) = g_0(X) + g_1(X)x + \cdots + g_m(X)x^m,$$

其中 $g_i(X) \in R[X]$．在 $S^{-1}R$ 中，有某个$s \in S$使得$x = h(s)^{-1}$，根据归纳假设，$g_i(X) = h(r_i)h(\sigma_i)^{-1}$，其中 $r_i \in R$ 和 $\sigma_i \in \overline{S}$．从而，

$$\begin{aligned} y &= h(r_0)h(\sigma_0)^{-1} + h(r_1)h(\sigma_1)^{-1}h(s)^{-1} + \cdots + h(r_m)h(\sigma_m)^{-1}h(s)^{-m} \\ &= h(s)^{-m}(h(r_0)h(\sigma_0)^{-1}h(s)^m + h(r_1)h(\sigma_1)^{-1}h(s)^{m-1} + \cdots + h(r_m)h(\sigma_m)^{-1}) \\ &= h(r')h(\sigma)^{-1}, \end{aligned}$$

其中 $r' \in R$ 和 $\sigma = \sigma_0\sigma_1\cdots\sigma_m s^m \in \overline{S}$．所以，$y = h(r')h(\sigma)^{-1}$． ■

依据命题 11.13，$S^{-1}R$ 的元素可以看作"分数"$h(r)h(\sigma)^{-1}$，其中 $r \in R$ 和 $\sigma \in \overline{S}$．

记号　设 $h: R \to S^{-1}R$ 是局部化映射．如果 $r \in R$ 和 $\sigma \in \overline{S}$，定义

$$r/\sigma = h(r)h(\sigma)^{-1}.$$

特别地，$r/1 = h(r)$．

局部化映射 $h: r \to r/1$ 是单射吗？最简单的例子是 $0 \in S$ 时 h 产生核（毕竟，S 允许是 R 的任意子集）．如果 0 可逆，则 $0 = 00^{-1} = 1$，从而 $S^{-1}R$ 是零环．于是，$h: R \to S^{-1}R$ 是零映射，因此它不是单射除非 R 是零环．下一命题研究 $\ker h$．

命题 11.14　如果 S 是交换环 R 的子集，又如果 $h: R \to S^{-1}R$ 是局部化映射，则

$$\ker h = \{r \in R: 有某个\ \sigma \in \overline{S}\ 使得\ \sigma r = 0\}.$$

证明　如果 $\sigma r = 0$，则在 $S^{-1}R$ 中，$0 = h(\sigma)h(r)$．因 $h(\sigma)$ 是单位，有 $0 = h(\sigma)^{-1}h(\sigma)h(r) = h(r)$，从而 $r \in \ker h$．

反之，假设在 $S^{-1}R$ 中 $h(r) = 0$．因 $S^{-1}R = R[X]/I$，其中 $I = \{sx_s - 1 : s \in S\}$，在 $R[X]$ 中有等式 $r = \sum_{i=1}^{n} f_i(X)(s_i x_{s_i} - 1)$．如果 $S_0 = \{s_1,\cdots,s_n\} \cup \{一切\ f_i(X)\ 的非零系数\}$ 和 $h_0: R \to (S_0)^{-1}R$ 是局部化映射，则 $r \in \ker h_0$．事实上，如果 $s = s_1\cdots s_n$ 和 $h': R \to \{s\}^{-1}R$ 是局部化映射，则每个 $h'(s_i)$ 是可逆的，这是因为 $s_i^{-1} = s^{-1}s_1\cdots\hat{s}_i\cdots s_n$．现在 $\{s\}^{-1}R = R[X]/(sx - 1)$，因此 $r \in \ker h'$ 表明存在 $f(x) = \sum_{i=0}^{m} a_i x^i$ 使得

$$在\ R[X]\ 中，r = f(x)(sx - 1) = \Big(\sum_{i=0}^{m} a_i x^i\Big)(sx - 1) = \sum_{i=0}^{m}(sa_i x^{i+1} - a_i x^i).$$

展开且由 x 的同次幂的系数相等得

$$r = -a_0, sa_0 = a_1, \cdots, sa_{m-1} = a_m, sa_m = 0.$$

因此，$sr = -sa_0 = -a_1$，由归纳法可知，对一切 i 有 $s^i r = -a_i$．特别地，$s^m r = -a_m$，从而正如所要的，$s^{m+1}r = -sa_m = 0$． ■

什么时候两个"分数"r/σ 和 r'/σ' 相等？

系 11.15　设 S 是交换环 R 的子集且 $0 \notin S$．如果 $r/\sigma, r'/\sigma' \in S^{-1}R$，其中 $\sigma, \sigma' \in \overline{S}$，则 $r/\sigma = r'/\sigma'$ 当且仅当存在 $\sigma'' \in \overline{S}$ 使得在 R 中有 $\sigma''(r\sigma' - r'\sigma) = 0$．

注　如果 S 不包含零因子，则因 σ'' 是单位，所以 $\sigma''(r\sigma' - r'\sigma) = 0$ 当且仅当 $r\sigma' - r'\sigma = 0$，即 $r\sigma' = r'\sigma$．

证明　如果 $r/\sigma = r'/\sigma'$，则乘以 $\sigma\sigma'$ 得 $S^{-1}R$ 中 $(r\sigma' - r'\sigma)/1 = 0$．因此，$r\sigma' - r'\sigma \in \ker h$，且命题 11.14 给出 $\sigma'' \in \overline{S}$ 使得在 R 中有 $\sigma''(r\sigma' - r'\sigma) = 0$.

反之，如果有某个 $\sigma'' \in \overline{S}$ 使得在 R 中有 $\sigma''(r\sigma' - r'\sigma) = 0$，则在 $S^{-1}R$ 中有 $h(\sigma'')h(r\sigma' - r'\sigma) = 0$. 由于 $h(\sigma'')$ 是单位，有 $h(r)h(\sigma') = h(r')h(\sigma)$；由于 $h(\sigma)$ 和 $h(\sigma')$ 是单位，有 $h(r)h(\sigma)^{-1} = h(r')h(\sigma')^{-1}$；即 $r/\sigma = r'/\sigma'$. ■

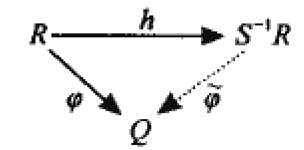
系 11.16 假定 $0 \notin S$，并设 S 是交换环 R 的子集.

(i) 如果 S 不包含零因子，则局部化映射 $h: R \to S^{-1}R$ 是单射.

(ii) 如果 R 是整环，且 $Q = \mathrm{Frac}(R)$，则 $S^{-1}R \subseteq Q$. 此外，如果 $S = R - \{0\}$，则 $S^{-1}R = Q$.

证明 (i) 容易从命题 11.14 得到.

(ii) 根据命题 11.14，局部化映射 $h: R \to S^{-1}R$ 是单射. 考虑图



其中 φ 是包含映射. 如果 $\tilde{\varphi}(h(r)h(\sigma)^{-1}) = 0$，则因 $h(\sigma)$ 是 $S^{-1}R$ 中的单位，所以 $\tilde{\varphi}(h(r)) = 0$. 但图的交换性给出 $\tilde{\varphi}h(r) = \varphi(r)$. 由于 φ 是单射，因此 $r = 0$；从而 $h(r)h(\sigma)^{-1} = 0$，所以 $\tilde{\varphi}$ 是单射. ■

作为系11.16(ii)的一个推论，当 R 是整环且 S 是不包含 0 的乘法封闭子集时，$S^{-1}R$ 由一切元素 $a/s \in \mathrm{Frac}(R)$ 组成，其中 $a \in R$ 和 $s \in S$.

我们现在研究 $S^{-1}R$ 中的理想.

定义 如果 S 是交换环 R 的子集，又如果 I 是 R 中的理想，则由 $h(I)$ 生成的 $S^{-1}R$ 中的理想记为 $S^{-1}I$.

例 11.17 (i) 如果 S 是交换环 R 的子集，又如果 I 是 R 中包含一个元素 $\sigma \in \overline{S}$ 的理想——即 $I \cap \overline{S} \neq \varnothing$，则 $S^{-1}I$ 包含 $\sigma/\sigma = 1$，从而 $S^{-1}I = S^{-1}R$.

(ii) 设 S 由一切奇整数组成 [即 S 是素理想(2)的补]，设 $I = (3)$，并设 $I' = (5)$. 则 $S^{-1}I = S^{-1}\mathbb{Z} = S^{-1}I'$. 所以，由 $I \mapsto S^{-1}I$ 给出的从 $\mathbb{Z}$ 中的理想到 $S^{-1}\mathbb{Z} = \mathbb{Z}_{(2)}$ 中的理想的函数不是单射. 在下一系中将会看到，当把我们只关注包含于 (2) 中的素理想时，情况得到改善. ■

系 11.18 设 S 是交换环 R 的子集.

(i) $S^{-1}R$ 中的每个理想 J 形如 $S^{-1}I$，其中 I 是 R 中的某个理想. 事实上，如果 R 是整环且 $I = J \cap R$，则 $J = S^{-1}I$；一般情形中，如果 $I = h^{-1}(h(R) \cap J)$，则 $J = S^{-1}I$.

(ii) 如果 I 是 R 中的理想，则 $S^{-1}I = S^{-1}R$ 当且仅当 $I \cap \overline{S} \neq \varnothing$.

(iii) 如果 $\mathfrak{q}$ 是 R 中的素理想且 $\mathfrak{q} \cap \overline{S} = \varnothing$ 则 $S^{-1}\mathfrak{q}$ 是 $S^{-1}R$ 中的素理想.

(iv) 从 R 中一切和 $\overline{S}$ 不交的素理想的族到 $\mathrm{Spec}(S^{-1}R)$ 的函数 $\mathfrak{q} \mapsto S^{-1}\mathfrak{q}$ 是双射.

(v) 如果 R 是诺特环，则 $S^{-1}R$ 也是诺特环.

证明 (i) 设 $J = (j_\lambda : \lambda \in \Lambda)$. 根据命题 11.14，有 $j_\lambda = h(r_\lambda)h(\sigma_\lambda)^{-1}$，其中 $r_\lambda \in R$ 和 $\sigma_\lambda \in \overline{S}$. 定义 I 为由 $(r_\lambda : \lambda \in \Lambda)$ 生成的 R 中的理想；即 $I = h^{-1}(h(R) \cap J)$. 显然 $S^{-1}I = J$；事实上，因一切 σ_λ 是 $S^{-1}R$ 中的单位，有 $J = (h(r_\lambda) : \lambda \in \Lambda)$.

(ii) 如果 $\sigma \in I \cap \overline{S}$，则 $\sigma/1 \in S^{-1}I$. 但 $\sigma/1$ 是 $S^{-1}R$ 中的单位. 从而 $S^{-1}I = S^{-1}R$. 反之，如果 $S^{-1}I = S^{-1}R$，则有某个 $a \in I$ 和 $\sigma \in \overline{S}$ 使得 $h(a)h(\sigma)^{-1} = 1$. 因此，$\sigma - a \in \ker h$，从而存在 $\sigma'' \in \overline{S}$ 使得 $\sigma''(\sigma - a) = 0$. 所以，$\sigma''\sigma = \sigma''a \in I$. 因 $\overline{S}$ 是乘法封闭的，$\sigma''\sigma \in I \cap \overline{S}$.

(iii) 假设 $\mathfrak{q}$ 是 R 中的素理想. 首先，因 $\mathfrak{q} \cap \overline{S} = \varnothing$，$S^{-1}\mathfrak{q}$ 是真理想. 如果 $(a/\sigma)(b/\tau) = \mathfrak{q}/\omega$，其中 $a, b \in R$ 和 $\sigma, \tau, \omega \in \overline{S}$，则存在 $\sigma'' \in \overline{S}$ 使得 $\sigma''(\omega ab - \sigma\tau\mathfrak{q}) = 0$. 因此，$\sigma''\omega ab \in \mathfrak{q}$. 现在 $\sigma''\omega \notin \mathfrak{q}$ (因

为 $\sigma''\omega \in \overline{S}$ 和 $\overline{S} \cap \mathfrak{q} = \varnothing$)；从而，$ab \in \mathfrak{q}$(因为 $\mathfrak{q}$ 是素的)．于是，不是 a 就是 b 在 $\mathfrak{q}$ 中，从而不是 a/σ 就是 b/τ 在 $S^{-1}\mathfrak{q}$ 中．所以，$S^{-1}\mathfrak{q}$ 是素理想．

(iv) 假设 $\mathfrak{p}$ 和 $\mathfrak{q}$ 都是 R 中的素理想，且 $S^{-1}\mathfrak{p} = S^{-1}\mathfrak{q}$；可以假定 $\mathfrak{p} \cap \overline{S} = \varnothing = \mathfrak{q} \cap \overline{S}$. 如果 $a \in \mathfrak{p}$，则存在 $b \in \mathfrak{q}$ 和 $\sigma \in \overline{S}$ 使得 $a/1 = b/\sigma$. 因此，$\sigma a - b \in \ker h$，其中 h 是局部化映射，从而存在 $\sigma' \in \overline{S}$ 使得 $\sigma'\sigma a = \sigma' b \in \mathfrak{q}$. 但 $\sigma'\sigma \in \overline{S}$，因此 $\sigma'\sigma \notin \mathfrak{q}$. 因 $\mathfrak{q}$ 是素的，必有 $a \in \mathfrak{q}$；即 $\mathfrak{p} \subseteq \mathfrak{q}$. 类似地可证明反包含．

设 $\mathfrak{P}$ 是 $S^{-1}R$ 中的素理想．根据 (i)，存在 R 中的某个理想 I 使得 $\mathfrak{P} = S^{-1}I$. 我们必须证明可以选取 I 为 R 中的素理想．现在 $h(R) \cap \mathfrak{P}$ 是 $h(R)$ 中的素理想，从而 $\mathfrak{p} = h^{-1}(h(R) \cap \mathfrak{P})$ 是 R 中的素理想．根据 (i)，$\mathfrak{P} = S^{-1}\mathfrak{p}$.

(v) 如果 J 是 $S^{-1}R$ 中的理想，则 (i) 证明有 R 中的某个理想 I 使得 $J = S^{-1}I$. 因 R 是诺特环，有 $I = (r_1, \cdots, r_n)$，从而 $J = (r_1/1, \cdots, r_n/1)$. 因此，$S^{-1}R$ 中的每个理想是有限生成的，所以 $S^{-1}R$ 是诺特环． ■

定义 如果 $\mathfrak{p}$ 是交换环 R 中的素理想，则补 $S = R - \mathfrak{p}$ 是乘法封闭的，记 $S^{-1}R$ 为 $R_{\mathfrak{p}}$.

例 11.19 如果 p 是 $\mathbb{Z}$ 中的素数，则 $\mathfrak{p} = (p)$ 是素理想，且 $\mathbb{Z}_{\mathfrak{p}} = \mathbb{Z}_{(p)}$. ■

命题 11.20 如果 R 是整环，则 $\bigcap_{\mathfrak{m}} R_{\mathfrak{m}} = R$，其中交遍历 R 中的一切极大理想 $\mathfrak{m}$.

证明 因 R 是整环，对一切 $\mathfrak{m}$，$R_{\mathfrak{m}} \subseteq \mathrm{Frac}(R)$，因此陈述中的交有定义．此外，易知对一切 $\mathfrak{m}$，$R \subseteq R_{\mathfrak{m}}$，因此 $R \subseteq \bigcap_{\mathfrak{m}} R_{\mathfrak{m}}$. 关于反包含，设 $a \in \bigcap R_{\mathfrak{m}}$. 定义

$$I = (R : a) = \{r \in R : ra \in R\}.$$

如果 $I = R$，则 $1 \in I$，正如所要的有 $a = 1a \in R$. 如果 I 是真理想，则存在极大理想 $\mathfrak{m}$ 使得 $I \subseteq \mathfrak{m}$. 现在 $a/1 \in R_{\mathfrak{m}}$，因此存在 $r \in R$ 和 $\sigma \notin \mathfrak{m}$ 使得 $a/1 = r/\sigma$；即 $\sigma a = r \in R$. 从而，$\sigma \in I \subseteq \mathfrak{m}$，与 $\sigma \notin \mathfrak{m}$ 矛盾．所以，$R = \bigcap_{\mathfrak{m}} R_{\mathfrak{m}}$. ■

下一命题说明为什么把 $S^{-1}R$ 叫做局部化．

命题 11.21 如果 $\mathfrak{p}$ 是交换环 R 中的素理想，则 $R_{\mathfrak{p}}$ 是有极大理想 $\mathfrak{p}R_{\mathfrak{p}} = \{r/s : r \in \mathfrak{p}$ 和 $s \notin \mathfrak{p}\}$ 的局部环．

证明 如果 $x \in R_{\mathfrak{p}}$，则 $x = r/s$，其中 $r \in R$ 和 $s \notin \mathfrak{p}$. 如果 $r \notin \mathfrak{p}$，则 r/s 是 $R_{\mathfrak{p}}$ 中的单位；即一切非单位在 $\mathfrak{p}R_{\mathfrak{p}}$ 中．因此，如果 I 是 $R_{\mathfrak{p}}$ 中的包含一个元素 r/s 的任一理想，其中 $r \notin \mathfrak{p}$，则 $I = R_{\mathfrak{p}}$. 由此 $R_{\mathfrak{p}}$ 中的每个真理想包含在 $\mathfrak{p}R_{\mathfrak{p}}$ 中，从而 $R_{\mathfrak{p}}$ 是有唯一极大理想 $\mathfrak{p}R_{\mathfrak{p}}$ 的局部环． ■

局部／整体策略潜在的基本假定是局部情形比整体简单．一般环上投射模的结构可能非常复杂，但下一命题证明局部环上的投射模是自由的．

引理 11.22 设 R 是有极大理想 $\mathfrak{m}$ 的局部环．元素 $r \in R$ 是单位当且仅当 $r \notin \mathfrak{m}$.

证明 显然，如果 r 是单位，则 $r \notin \mathfrak{m}$，这是因为 $\mathfrak{m}$ 是真理想．反之，假定 r 不是单位．根据佐恩引理，存在极大理想包含主理想 (r). 因 R 是局部的，只有一个极大理想，就是 $\mathfrak{m}$，因此，$r \in \mathfrak{m}$. ■

命题 11.23 如果 R 是局部环，则每个有限生成[⊖]投射 R-模 B 是自由的．

证明 设 R 是有极大理想 $\mathfrak{m}$ 的局部环，并设 $\{b_1, \cdots, b_n\}$ 是 B 的生成元的极小集；即 B 不能由

⊖ 卡普兰斯基的一个定理可以去掉有限性的假设：局部环上的每个投射模是自由的．他甚至证明了当 R 是非交换局部环时的自由性．

少于 n 个元素生成．设 F 是以 $x_1,\cdots,x_n$ 为基的自由 R-模，定义 $\varphi: F\to B$ 为对一切 i，$\varphi(x_i)=b_i$．于是，存在正合列

$$0\to K\to F\xrightarrow{\varphi} B\to 0, \tag{1}$$

其中 $K=\ker\varphi$．

我们断言 $K\subseteq \mathfrak{m}F$．如果相反，$K\nsubseteq \mathfrak{m}F$，则存在元素 $y=\sum_{i=1}^{n} r_i x_i\in K$，它不在 $\mathfrak{m}F$ 中；即某个系数，比如 $r_1\notin \mathfrak{m}$．现在根据引理 11.22，r_1 是单位．而 $y\in K=\ker\varphi$ 给出 $y=\sum r_i b_i=0$．因此，$b_1=-r_1^{-1}\left(\sum_{i=2}^{n} r_i b_i\right)$，这蕴涵 $B=\langle b_2,\cdots,b_n\rangle$，和原始生成集的极小性矛盾．

回到正合列 (1)，B 的投射性给出 $F=K\oplus B'$，其中 B' 是 F 的子模且 $B'\cong B$．因此，$\mathfrak{m}F=\mathfrak{m}K\oplus \mathfrak{m}B'$．因 $\mathfrak{m}K\subseteq K\subseteq \mathfrak{m}F$，系 7.18 给出

$$K=\mathfrak{m}K\oplus(K\cap \mathfrak{m}B').$$

但 $K\cap \mathfrak{m}B'\subseteq K\cap B'=\{0\}$，从而 $K=\mathfrak{m}K$．子模 K 是有限生成的，它是有限生成模 F 的直和项（因此是一个同态象），从而 Nakayama 引理（系 8.32）给出 $K=\{0\}$．所以，φ 是同构且 B 是自由的． ■

对交换环进行了局部化后，我们现在对它的模进行局部化．如果 M 是 R-模和 $s\in R$，令 μ_s 表示由 $m\mapsto sm$ 定义的乘映射．注意，如果 S 是 R 的子集，则 $\mu_s: M\to M$ 可逆当且仅当 M 是一个 $S^{-1}R$-模．

定义 设 R 是交换环并设 S 是 R 的任一子集．R-模 M 的**局部化**是指一个 $S^{-1}R$-模 $S^{-1}M$（即 $\mu_s: S^{-1}M\to S^{-1}M$ 对一切 $s\in S$ 都是可逆的）和一个叫做**局部化映射**的 R-映射 $h_M: M\to S^{-1}M$，它是下面泛映射问题的解：

$$\begin{array}{ccc} M & \xrightarrow{h} & S^{-1}M \\ & \searrow^{\varphi} \quad \swarrow_{\widetilde{\varphi}} & \\ & M' & \end{array}$$

如果 $\varphi: M\to M'$ 是 R-映射，其中 M' 是 $S^{-1}R$-模，则存在唯一 $S^{-1}R$-映射 $\widetilde{\varphi}: S^{-1}M\to M'$ 使得图交换．

$S^{-1}M$ 的明显的候选者——即 $S^{-1}R\otimes_R M$ ——事实上是它的局部化．

命题 11.24 设 R 是交换环，设 S 是 R 的任意子集，并设 M 是 R-模．则 $S^{-1}R\otimes_R M$ 和由 $m\mapsto 1\otimes m$ 给出的 R-映射 $h: M\to S^{-1}R\otimes_R M$ 是 M 的局部化．

证明 设 $\varphi: M\to M'$ 是 R-映射，其中 M' 是 $S^{-1}R$-模．易知定义为 $(r/\sigma, m)\mapsto (r/\sigma)\varphi(m)$ 的函数 $S^{-1}R\times M\to M'$（其中 $r\in R$ 和 $\sigma\in \overline{S}$）是 R-双线性函数．因此，存在唯一的 R-映射 $\widetilde{\varphi}: S^{-1}R\otimes_R M\to M'$ 使得 $\widetilde{\varphi}h=\varphi$．因 $h(M)$ 生成 $S^{-1}R\otimes_R M$，$\widetilde{\varphi}$ 是唯一的 R-映射使得图交换．我们让读者验证 $\widetilde{\varphi}$ 是 $S^{-1}R$-映射． ■

$S^{-1}R$ 的最重要的性质之一是它作为 R-模是平坦的．为了给出证明，我们先推广命题 11.14 中的论证．

命题 11.25 如果 S 是交换环 R 的子集，M 是 R-模，又如果 $h_M: M\to S^{-1}M$ 是局部化映

射，则

$$\ker h_M = \{m \in M: 有某个\ \sigma \in \overline{S}\ 使得\ \sigma m = 0\}.$$

证明 记 $\{m \in M: 有某个\ \sigma \in \overline{S}\ 使得\ \sigma m = 0\}$ 为 K. 如果对某个 $m \in M$ 和 $\sigma \in \overline{S}$，$\sigma m = 0$，则 $h_M(m) = (1/\sigma)h_M(\sigma m) = 0$，从而 $K \subseteq \ker h_M$. 关于反包含，和命题 11.14 一样进行：如果 $m \in K$，存在 $\sigma \in \overline{S}$ 使得 $\sigma m = 0$. 简化为关于某个 $\sigma \in \overline{S}$，$S = \{\sigma\}$ 的情形，由此 $S^{-1}R = R[x]/(\sigma x - 1)$. 现在因为 $R[x]$ 是以 $\{1, x, x^2, \cdots\}$ 为基的自由 R-模，所以 $R[x] \otimes_R M \cong \sum_i Rx^i \otimes_R M$. 因此，$R[x] \otimes_R M$ 中的每个元素有形如 $\sum_i x^i \otimes_R m_i$ 的唯一表达式，其中 $m_i \in M$. 特别地，如果 $m \in \ker h_M$，则

$$0 = 1 \otimes m = (\sigma x - 1)\sum_{i=0}^{n} x^i \otimes m_i = \sum_{i=0}^{n}(\sigma x^{i+1} \otimes m_i - x^i \otimes m_i).$$

现在证明可以像命题 11.14 的证明一样完成. 展开且由系数相等得等式

$$1 \otimes m = -1 \otimes m_0, x \otimes \sigma m_0 = x \otimes m_1, \cdots,$$
$$x^n \otimes \sigma m_{n-1} = x^n \otimes m_n, x^{n+1} \otimes \sigma m_n = 0.$$

由此

$$m = -m_0, \sigma m_0 = m_1, \cdots \sigma m_{n-1} = m_n, \sigma m_n = 0.$$

因此，$\sigma m = -\sigma m_0 = -m_1$，由归纳法可知对一切 i，$\sigma^i m = -m_i$. 特别地，$\sigma^n m = -m_n$，从而在 M 中 $\sigma^{n+1} m = -\sigma m_n = 0$. 所以正如所要的有 $\ker h_M \subseteq K$. ■

系 11.26 设 S 是交换环 R 的子集并设 M 是 R-模.

(i) 对每个元素 $u \in S^{-1}M$，有某个 $\sigma \in \overline{S}$ 和某个 $m \in M$ 使得 u 有 $u = \sigma^{-1}m$ 的形式.

(ii) 在 $S^{-1}M$ 中 $s_1^{-1}m_1 = s_2^{-1}m_2$ 当且仅当有某个 $\sigma \in \overline{S}$ 使得在 M 中 $\sigma(s_1^{-1}m_1 - s_2^{-1}m_2) = 0$.

证明 (i) 如果 $u \in S^{-1}M$，则 $u = \sum_i (r_i/\sigma_i)m_i$，其中 $r_i \in R$，$\sigma_i \in \overline{S}$，$m_i \in M$. 如果定义 $\sigma = \Pi\sigma_i$ 和 $\hat{\sigma}_i = \prod_{j \neq i}\sigma_j$，则

$$\begin{aligned} u &= \sum (1/\sigma_i)r_i m_i \\ &= \sum (\hat{\sigma}_i/\sigma)r_i m_i \\ &= (1/\sigma)\sum \hat{\sigma}_i r_i m_i \\ &= (1/\sigma)m, \end{aligned}$$

其中 $m = \sum\hat{\sigma}_i r_i m_i \in M$.

(ii) 如果 $\sigma \in \overline{S}$ 使得在 M 中 $\sigma(s_2 m_1 - s_1 m_2) = 0$，则在 $S^{-1}M$ 中 $(\sigma/1)(s_2 m_1 - s_1 m_2) = 0$. 由于 $\sigma/1$ 是单位，$s_2 m_1 - s_1 m_2 = 0$，从而 $s_1^{-1}m_1 = s_2^{-1}m_2$.

反之，如果在 $S^{-1}M$ 中 $s_1^{-1}m_1 = s_2^{-1}m_2$，则 $(1/s_1 s_2)(s_2 m_1 - s_1 m_2) = 0$. 因 $1/s_1 s_2$ 是单位，有 $(s_2 m_1 - s_1 m_2) = 0$ 和 $s_2 m_1 - s_1 m_2 \in \ker h_M$. 根据命题 11.25，存在 $\sigma \in \overline{S}$ 使得在 M 中 $\sigma(s_2 m_1 - s_1 m_2) = 0$. ■

系 11.27 设 S 是交换环 R 的子集. 如果 A 是 $S^{-1}R$-模，则 $A \cong S^{-1}A$.

证明 定义 $\varphi: A \to S^{-1}A$ 为 $a \mapsto 1 \otimes a$. 如果 $\varphi(a) = 0$，则存在 $\sigma \in \overline{S}$ 使得 $\sigma a = 0$. 因 σ 是 $S^{-1}R$ 中的单位且 A 是 $S^{-1}R$-模，等式 $a = \sigma^{-1}\sigma a = 0$ 在 A 中有意义. 因此，φ 是单射. 为证明 φ 是满射，注意 $(1/\sigma) \otimes a = \varphi(\sigma^{-1}a)$. ■

定理 11.28 如果 S 是交换环 R 的子集，则 $S^{-1}R$ 是平坦 R-模．

证明 需要证明如果 $0 \to A \xrightarrow{f} B$ 是正合的，则

$$0 \to S^{-1}R \otimes_R A \xrightarrow{1 \otimes f} S^{-1}R \otimes_R B$$

也是正合的．设 $u \in \ker(1 \otimes f)$；根据系 11.26，有某个 $\sigma \in \overline{S}$ 和 $a \in A$ 使得 $u = \sigma^{-1} \otimes a$．现在 $0 = (1 \otimes f)(u) = \sigma^{-1} \otimes f(a)$，从而 $f(a) \in \ker h_B$．根据命题 11.25，存在 $\tau \in \overline{S}$ 使得 $0 = \tau f(a) = f(\tau a)$．于是，因为 f 是单射，$\tau a \in \ker f = \{0\}$．所以，$0 = 1 \otimes \tau a = \tau(1 \otimes a) = \tau u$．最后，因 τ 是单位，有 $u = 0$．所以，$1 \otimes f$ 是单射，从而 $S^{-1}R$ 是平坦 R-模． ■

系 11.29 如果 S 是交换环 R 的子集，则局部化 $M \mapsto S^{-1}M = S^{-1}R \otimes_R M$ 定义了一个正合函子 ${}_R\mathbf{Mod} \to {}_{S^{-1}R}\mathbf{Mod}$．

证明 局部化是函子 $S^{-1}R \otimes_R$，它是正合的是因为 $S^{-1}R$ 是平坦 R-模． ■

记号 在 $S = R - \mathfrak{p}$ 的特殊情形中，其中 $\mathfrak{p}$ 是 R 中的素理想，我们记

$$S^{-1}M = M_{\mathfrak{p}}.$$

如果 $f: M \to N$ 是 R-映射，记 $f_{\mathfrak{p}}: M_{\mathfrak{p}} \to N_{\mathfrak{p}}$，其中 $f_{\mathfrak{p}} = 1_{R_{\mathfrak{p}}} \otimes f$．

我们用这个记号重述系 11.18（iv）．函数 $\mathfrak{q} \mapsto \mathfrak{q}_{\mathfrak{p}}$ 是 R 中包含在 $\mathfrak{p}$ 中的一切素理想的族到 $\operatorname{Spec}(R_{\mathfrak{p}})$ 的双射（见习题 6.67）．

下面是一些整体化结果．

命题 11.30 设 I 和 J 是整环 R 中的理想．如果对每个极大理想 $\mathfrak{m}$，$I_{\mathfrak{m}} = J_{\mathfrak{m}}$，则 $I = J$．

证明 取 $b \in J$，并定义

$$(I : b) = \{r \in R : rb \in I\}.$$

设 $\mathfrak{m}$ 是 R 中的一个极大理想．因 $I_{\mathfrak{m}} = J_{\mathfrak{m}}$，存在 $a \in I$ 和 $s \notin \mathfrak{m}$ 使得 $b/1 = a/s$．因 R 是整环，$sb = a \in I$，从而 $s \in (I : b)$；但 $s \notin \mathfrak{m}$，从而 $(I : b) \nsubseteq \mathfrak{m}$．因为 $(I : b)$ 不包含在任意极大理想之中，它不可能是真理想．所以 $(I : b) = R$；因此，$1 \in (I : b)$ 且 $b = 1b \in I$．我们已经证明了 $J \subseteq I$，对于反包含可类似地证明． ■

命题 11.31 设 R 是交换环．

（i）如果 M 是 R-模，且对每个极大理想 $\mathfrak{m}$ 有 $M_{\mathfrak{m}} = \{0\}$，则 $M = \{0\}$．

（ii）如果 $f: M \to N$ 是 R-映射且对每个极大理想 $\mathfrak{m}$，$f_{\mathfrak{m}}: M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ 是单射，则 f 是单射．

（iii）如果 $f: M \to N$ 是 R-映射且对每个极大理想 $\mathfrak{m}$，$f_{\mathfrak{m}}: M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ 是满射，则 f 是满射．

（iv）如果 $f: M \to N$ 是 R-映射且对每个极大理想 $\mathfrak{m}$，$f_{\mathfrak{m}}: M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ 是同构，则 f 是同构．

证明 （i）如果 $M \neq \{0\}$，则存在 $m \in M$ 且 $m \neq 0$．由此零化子 $I = \{r \in R : rm = 0\}$ 是 R 中的真理想，这是因为 $1 \notin I$，从而存在某个极大理想 $\mathfrak{m}$ 包含 I．现在在 $M_{\mathfrak{m}}$ 中 $1 \otimes m = 0$，从而 $m \in \ker h_M$．因为 $R - \mathfrak{m}$ 是乘法封闭的，命题 11.25 给出 $s \notin \mathfrak{m}$ 使得在 M 中 $sm = 0$．因此，$s \in I \subseteq \mathfrak{m}$，这是一个矛盾．所以 $M = \{0\}$．

（ii）存在正合列 $0 \to K \to M \xrightarrow{f} N$，其中 $K = \ker f$．因局部化是正合函子，对每个极大理想 $\mathfrak{m}$，存在正合列

$$0 \to K_{\mathfrak{m}} \to M_{\mathfrak{m}} \xrightarrow{f_{\mathfrak{m}}} N_{\mathfrak{m}}.$$

根据假设，每个 $f_{\mathfrak{m}}$ 是单射，因此对一切极大理想 $\mathfrak{m}$，$K_{\mathfrak{m}} = \{0\}$．现在（i）证明 $K = \{0\}$，从而 f 是单射．

（ⅲ）存在正合列 $M \xrightarrow{f} N \to C \to 0$，其中 $C = \operatorname{coker} f = N/\operatorname{im} f$．因张量积是右正合的，对一切极大理想 $\mathfrak{m}$，$C_{\mathfrak{m}} = \{0\}$，因此 $C = \{0\}$．但 f 是满射当且仅当 $C = \operatorname{coker} f = \{0\}$．

（ⅳ）从（ⅱ）和（ⅲ）立即可得．■

我们不能把命题11.31（ⅳ）的假设减弱为对一切极大理想 $\mathfrak{m}$，$M_{\mathfrak{m}} \cong N_{\mathfrak{m}}$，必须假定由给定的映射 $f: M \to N$ 形成一切局部同构．如果 G 是 $\mathbb{Q}$ 的子群，它由一切 a/b 组成，其中 b 无平方因数，则在例 11.5 中可知对一切素数 p，$G_{(p)} \cong \mathbb{Z}_{(p)}$，但 $G \ncong \mathbb{Z}$．

习题 11.20 和习题 11.22 证明局部化保持投射和平坦；即如果 A 是投射 R-模，则 $S^{-1}A$ 是投射 $(S^{-1}R)$-模，如果 B 是平坦 R-模，则 $S^{-1}B$ 是平坦 $(S^{-1}R)$-模．保持内射性比较深奥．

引理 11.32 *设 S 是交换环 R 的子集，并设 M 和 A 是 R-模，其中 A 有有限表现．则存在自然同构*

$$\tau_A : S^{-1}\operatorname{Hom}_R(A, M) \to \operatorname{Hom}_{S^{-1}R}(S^{-1}A, S^{-1}M).$$

证明 只需构造自然同构

$$\theta_A : \operatorname{Hom}_R(A, S^{-1}M) \to \operatorname{Hom}_{S^{-1}R}(S^{-1}A, S^{-1}M)$$

和

$$\varphi_A : S^{-1}\operatorname{Hom}_R(A, M) \to \operatorname{Hom}_R(A, S^{-1}M),$$

然后我们可以定义 $\tau_A = \theta_A \varphi_A$．

首先假定 $A = R^n$ 是有限生成自由 R-模．如果 $a_1, \cdots, a_n$ 是 A 的基，则 $a_1/1, \cdots, a_n/1$ 是 $S^{-1}A = S^{-1}R \otimes_R R^n$ 的基．易知由 $f \mapsto \tilde{f}$（其中 $\tilde{f}(a_i/\sigma) = f(a_i)/\sigma$）给出的映射

$$\theta_{R^n} : \operatorname{Hom}_R(A, S^{-1}M) \to \operatorname{Hom}_{S^{-1}R}(S^{-1}A, S^{-1}M)$$

是合理定义的 R-同构．

现在，如果 A 是有限表现的 R-模，则存在正合列

$$R^t \to R^n \to A \to 0. \tag{2}$$

运用反变函子 $\operatorname{Hom}_R(\ , M')$ 和 $\operatorname{Hom}_{S^{-1}R}(\ , M')$，其中 $M' = S^{-1}M$ 先看作 R-模，得到行正合的交换图

$$\begin{array}{ccccccc}
0 \to & \operatorname{Hom}_R(A, M') & \longrightarrow & \operatorname{Hom}_R(R^n, M') & \longrightarrow & \operatorname{Hom}_R(R^t, M') \\
& \Big\downarrow \theta_A & & \Big\downarrow \theta_{R^n} & & \Big\downarrow \theta_{R^t} \\
0 \to & \operatorname{Hom}_{S^{-1}R}(S^{-1}A, M') & \longrightarrow & \operatorname{Hom}_{S^{-1}R}((S^{-1}R)^n, M') & \longrightarrow & \operatorname{Hom}_{S^{-1}R}((S^{-1}R)^t, M')
\end{array}$$

因垂直映射 θ_{R^n} 和 θ_{R^t} 是同构，存在虚线箭头 θ_A，根据命题 8.94，它必是同构．如果 $\beta \in \operatorname{Hom}_R(A, M)$，则读者可以验证

$$\theta_A(\beta) = \tilde{\beta} : a/\sigma \mapsto \beta(a)/\sigma,$$

由此，同构 θ_A 是自然同构．

通过定义 $\varphi_A : g/\sigma \mapsto g_\sigma$ 来构造 $\varphi_A : S^{-1}\operatorname{Hom}_R(A, M) \to \operatorname{Hom}_R(A, S^{-1}M)$，其中 $g_\sigma(a) = g(a)/\sigma$．注意，因 φ_A 是由 $(r/\sigma, g) \mapsto rg_\sigma$ 给出的 R-双线性函数 $S^{-1}R \times \operatorname{Hom}_R(A, M) \to \operatorname{Hom}_R(A, S^{-1}M)$ 形成的，所以 φ_A 是合理定义的（记住 $S^{-1}\operatorname{Hom}_R(A, M) = S^{-1}R \otimes_R \operatorname{Hom}_R(A, M)$）．当 A 是有限生成自由模时，φ_A 是同构，考虑交换图

$$\begin{array}{ccccccc} 0 \longrightarrow & S^{-1}\mathrm{Hom}_R(A,M) & \longrightarrow & S^{-1}\mathrm{Hom}_R(R'',M) & \longrightarrow & S^{-1}\mathrm{Hom}_R(R',M) \\ & \downarrow{\scriptstyle \varphi_A} & & \downarrow{\scriptstyle \varphi_{R''}} & & \downarrow{\scriptstyle \varphi_{R'}} \\ 0 \longrightarrow & \mathrm{Hom}_R(A,S^{-1}M) & \longrightarrow & \mathrm{Hom}_R(R'',S^{-1}M) & \longrightarrow & \mathrm{Hom}_R(R',S^{-1}M) \end{array}$$

顶上一行是对(2)式先运用左正合反变函子 $\mathrm{Hom}_R(\ ,M)$ 再运用正合局部化函子形成的，所以它是正合的．底下一行是对(2)式运用左正合反变函子 $\mathrm{Hom}_R(\ ,S^{-1}M)$ 形成的，所以它也是正合的．习题 8.52 的五项引理表明 φ_A 是同构． ■

例 11.33 如果 A 不是有限表现的，引理 11.32 可能不成立．例如，设 $R=\mathbb{Z}$ 和 $S^{-1}R=\mathbb{Q}$．我们断言

$$\mathbb{Q}\otimes_{\mathbb{Z}}\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z})\not\cong\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}\otimes_{\mathbb{Z}}\mathbb{Q},\mathbb{Q}\otimes_{\mathbb{Z}}\mathbb{Z}).$$

因为 $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z})=\{0\}$，所以左端为 $\{0\}$．另一方面，右端是 $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Q})\cong\mathbb{Q}$． ■

命题 11.34 如果 S 是交换诺特环 R 的子集，又如果 E 是内射 R-模，则 $S^{-1}E$ 是内射 $(S^{-1}R)$-模．

注 如果 R 不是诺特环，这个结果可能不成立．如果 k 是域和 $R=k[X]$，其中 X 是不可数变量集，则存在内射 R-模 E 和 R 的子集 S 使得 $S^{-1}E$ 不是内射 $(S^{-1}R)$-模（见 E. C. Dade, "Localization of Injective Modules", *Journal of Algebra* 69 (1981), 416～425）．

证明 根据定理 7.68，即白尔判别法，只需证明

$$i^*:\mathrm{Hom}_{S^{-1}R}(S^{-1}R,S^{-1}E)\to\mathrm{Hom}_{S^{-1}R}(J,S^{-1}E)$$

对 $S^{-1}R$ 中的每个理想 J 都是满射，其中 $i:J\to S^{-1}R$ 是包含映射．现在根据系 11.18，$S^{-1}R$ 中的每个理想 J 形如 $J=S^{-1}I$，其中 I 是 R 中的理想．因 R 是诺特环，每个理想都是一个有限表现 R-模，从而运用引理 11.32 得垂直箭头是同构的交换图

$$\begin{array}{ccc} S^{-1}\mathrm{Hom}_R(R,E) & \longrightarrow & S^{-1}\mathrm{Hom}_R(I,E) \\ \downarrow{\scriptstyle \tau_R} & & \downarrow{\scriptstyle \tau_I} \\ \mathrm{Hom}_{S^{-1}R}(S^{-1}R,S^{-1}E) & \xrightarrow{i^*} & \mathrm{Hom}_{S^{-1}R}(S^{-1}I,S^{-1}E) \end{array}$$

E 的内射性蕴涵 $\mathrm{Hom}_R(R,E)\to\mathrm{Hom}_R(I,E)$ 是满射（其中的箭头是由包含映射 $I\to R$ 诱导的），从而局部化的正合性证明顶上一行的箭头是满射．因垂直箭头是同构，从而底下一行的箭头是满射．所以，$J=S^{-1}I$ 是内射 $(S^{-1}R)$-模． ■

局部化和 Tor 可交换，其原因本质上归咎于 $S^{-1}R$ 是一个平坦 R-模．

命题 11.35 如果 S 是交换环 R 的子集，则对一切 $n\geqslant 0$ 和一切 R-模 A 和 B，存在同构

$$S^{-1}\mathrm{Tor}_n^R(A,B)\cong\mathrm{Tor}_n^{S^{-1}R}(S^{-1}A,S^{-1}B).$$

证明 先考虑 $n=0$ 的情形．对固定的 R-模 A，存在自然同构

$$\tau_B:S^{-1}(A\otimes_R B)\to S^{-1}A\otimes_{S^{-1}R}S^{-1}B,$$

这是因为两者都是泛映射问题

$$\begin{array}{ccc} S^{-1}A\times S^{-1}B & \longrightarrow & U \\ & {\scriptstyle f}\searrow & \swarrow{\scriptstyle \tilde f} \\ & M & \end{array}$$

的解 U，其中 M 是 $(S^{-1}R)$-模，f 是 $(S^{-1}R)$-双线性函数，$\tilde f$ 是 $(S^{-1}R)$-映射．

如果 $\mathbf{P}_B$ 是 B 的删除投射分解，则局部化的正合性连同局部化保持投射证明 $S^{-1}(\mathbf{P}_B)$ 是 $S^{-1}B$

的删除投射分解．同构 τ_A 的自然性给出复形的同构

$$S^{-1}(A\otimes_R \mathbf{P}_B)\cong S^{-1}A\otimes_{S^{-1}R}S^{-1}(\mathbf{P}_B),$$

从而它们的同调群同构．因局部化是正合函子，适用命题 10.38，因此

$$H_n(S^{-1}(A\otimes_R \mathbf{P}_B))\cong S^{-1}H_n(A\otimes_R \mathbf{P}_B)\cong S^{-1}\mathrm{Tor}_n^R(A,B).$$

另一方面，因 $S^{-1}(\mathbf{P}_B)$ 是 $S^{-1}B$ 的删除投射分解，Tor 的定义给出

$$H_n(S^{-1}A\otimes_{S^{-1}R}S^{-1}(\mathbf{P}_B))\cong \mathrm{Tor}_n^{S^{-1}R}(S^{-1}A,S^{-1}B).$$ ■

系 11.36 设 A 是交换环 R 上的 R-模．如果对每个极大理想 $\mathfrak{m}$，$A_\mathfrak{m}$ 是平坦 $R_\mathfrak{m}$-模，则 A 是平坦 R-模．

证明 命题假设连同命题 10.96 给出对一切 $n\geqslant 1$，对每个 R-模 B 和每个极大理想 $\mathfrak{m}$，$\mathrm{Tor}_n^{R_\mathfrak{m}}(A_\mathfrak{m},B_\mathfrak{m})=\{0\}$．但命题 11.35 给出对一切极大理想 $\mathfrak{m}$ 和一切 $n\geqslant 1$，$\mathrm{Tor}_n^R(A,B)_\mathfrak{m}=\{0\}$．最后，命题 11.31 证明对一切 $n\geqslant 1$，$\mathrm{Tor}_n^R(A,B)=\{0\}$．因为该等式对一切 R-模 B 成立，所以 A 是平坦的． ■

对 Ext 我们必须附加一些假设才能得到类似的结果（见习题 11.23）．

引理 11.37 如果 R 是左诺特环和 A 是有限生成左 R-模，则存在 A 的投射分解 $\mathbf{P}_\bullet$，其中每个 P_n 是有限生成的．

证明 因 A 是有限生成的，存在有限生成自由左 R-模 P_0 和满射 R-映射 $\varepsilon:P_0\to A$．因 R 是左诺特环，$\ker\varepsilon$ 是有限生成的，从而存在有限生成自由左 R-模 P_1 和满射 R-映射 $d_1:P_1\to\ker\varepsilon$．如果定义 $D_1:P_1\to P_0$ 为复合 id_1，其中 $i:\ker\varepsilon\to P_0$ 是包含映射，则存在正合列

$$0\to\ker D_1\to P_1\xrightarrow{D_1}P_0\xrightarrow{\varepsilon}A\to 0.$$

因为 $\ker D_1$ 是有限生成的，这个构造可以迭代，从而证明可以由归纳法完成．（事实上我们构造了 A 的一个自由分解．） ■

命题 11.38 设 S 是交换诺特环 R 的子集．如果 A 是有限生成 R-模，则对一切 $n\geqslant 0$ 和一切 R-模 B，存在同构

$$S^{-1}\mathrm{Ext}_R^n(A,B)\cong \mathrm{Ext}_{S^{-1}R}^n(S^{-1}A,S^{-1}B).$$

证明 因 R 是诺特环和 A 是有限生成的，引理 11.37 表明存在 A 的投射分解 $\mathbf{P}$，它的每个项都是有限生成的．根据引理 11.32，对每个 R-模 B，存在自然同构

$$\tau_A:S^{-1}\mathrm{Hom}_R(A,B)\to \mathrm{Hom}_{S^{-1}R}(S^{-1}A,S^{-1}B)$$

（诺特环上的有限生成模必是有限表现的）．现在 τ_A 给出复形的同构

$$S^{-1}(\mathrm{Hom}_R(\mathbf{P}_A,B))\cong \mathrm{Hom}_{S^{-1}R}(S^{-1}(\mathbf{P}_A),S^{-1}B).$$

左端取同调得

$$H_n(S^{-1}(\mathrm{Hom}_R(\mathbf{P}_A,B)))\cong S^{-1}H_n(\mathrm{Hom}_R(\mathbf{P}_A,B))\cong S^{-1}\mathrm{Ext}_R^n(A,B),$$

这是因为局部化是正合函子（命题 10.38）．另一方面，右端的同调是

$$H_n(\mathrm{Hom}_{S^{-1}R}(S^{-1}(\mathbf{P}_A),S^{-1}B))=\mathrm{Ext}_{S^{-1}R}^n(S^{-1}A,S^{-1}B),$$

这是因为 $S^{-1}(\mathbf{P}_A)$ 是 $S^{-1}A$ 的 $(S^{-1}R)$-投射分解． ■

注 命题 11.38 的另一个证明可以用第二个变量的删除内射分解 $\mathbf{E}_B$．为了运用引理 11.32，仍然必须假定 A 是有限生成的，但现在所用的事实是：当 R 是诺特环时，局部化保持内射．

系 11.39 设 A 是交换诺特环 R 上的有限生成 R-模．则对每个极大理想 $\mathfrak{m}$，$A_{\mathfrak{m}}$ 是投射 $R_{\mathfrak{m}}$-模当且仅当 A 是投射 R-模．

证明 充分性是习题 11.20，必要性来自命题 11.38：对每个 R-模 B 和极大理想 $\mathfrak{m}$，有

$$\mathrm{Ext}_R^1(A,B)_{\mathfrak{m}} \cong \mathrm{Ext}_{R_{\mathfrak{m}}}^1(A_{\mathfrak{m}},B_{\mathfrak{m}}) = \{0\},$$

这是因为 $A_{\mathfrak{m}}$ 是投射的．根据命题 11.31，$\mathrm{Ext}_R^1(A,B) = \{0\}$，这说明 A 是投射的． ■

习题

11.1 证明作为 $\mathbb{Z}_{(p)}$-模，$\mathbb{Z}_{(p)} \not\cong \mathbb{Q}$．

11.2 如果 R 是整环且 $Q = \mathrm{Frac}(R)$，证明 Q 的每个 R-子代数 A 都是 R 的一个局部化．

提示：定义 $S = \{b \in R : 1/b \in A\}$．

该题是错的，给出一个反例.

11.3 证明对秩为 1 的无挠阿贝尔群 G，下面的陈述等价．

(i) G 是有限生成的．

(ii) G 是循环的．

(iii) 如果 $x \in G$ 非零，则对几乎一切 p，$h_p(x) = 0$，而对一切素数 p，$h_p(x) \neq \infty$．

(iv) $\tau(G) = \tau(\mathbb{Z})$.

11.4 (i) 如果 G 是秩为 1 的无挠阿贝尔群，证明 $\mathrm{End}(G)$ 的加法群是无挠的且秩为 1.

(ii) 设 $x \in G$ 非零，且 $\chi(x) = (h_2(x), h_3(x), \cdots, h_p(x), \cdots)$，并设 R 是 $\mathbb{Q}$ 的子环，其中 $\chi(1) = (k_2, k_3, \cdots, k_p, \cdots)$ 和

$$k_p = \begin{cases} \infty & \text{如果 } h_p(x) = \infty \\ 0 & \text{如果 } h_p(x) \text{ 有限}. \end{cases}$$

证明 $\mathrm{End}(G) \cong R$．证明存在无限个 G 使得 $\mathrm{Aut}(G) \cong \mathbb{I}_2$．

11.5 设 G 和 H 都是秩为 1 的无挠阿贝尔群．

(i) 证明 $G \otimes_{\mathbb{Z}} H$ 是无挠的且秩为 1.

(ii) 如果 (h_p) 是非零元素 $x \in G$ 的高度序列，又如果 (k_p) 是非零元素 $y \in H$ 的高度序列，证明 $x \otimes y$ 的高度序列是 (m_p)，其中 $m_p = h_p + k_p$（我们约定 $\infty + k_p = \infty$）．

11.6 设 T 是一切型的集合，对 $\tau, \tau' \in T$，如果存在高度序列 $(k_p) \in \tau$ 和 $(k'_p) \in \tau'$ 满足对一切素数 p 有 $k_p \leqslant k'_p$，则定义 $\tau \leqslant \tau'$．

(i) 证明 $\leqslant$ 是 T 上的偏序．

(ii) 证明：如果 G 和 G' 都是秩为 1 的无挠阿贝尔群，则 $\tau(G) \leqslant \tau(G')$ 当且仅当 G 和 G' 的一个子群同构．

(iii) 证明 T 是格，并证明：如果 $\tau = \tau(G)$ 和 $\tau' = \tau(G)$，则 $\tau \wedge \tau' = \tau(G \cap G')$ 和 $\tau \vee \tau' = \tau(G + G')$．

(iv) 如果 G 和 G' 都是秩为 1 的无挠阿贝尔群，证明 $\mathrm{Hom}(G,G') \neq \{0\}$ 当且仅当 $\tau(G) \leqslant \tau(G')$．

11.7 如果 G 是 p-准素阿贝尔群，证明 G 是 $\mathbb{Z}_{(p)}$-模．

11.8 如果 S 是交换环 R 的子集，又如果 $\overline{S}$ 是由 S 生成的乘法封闭子集，证明 $(\overline{S})^{-1}R \cong S^{-1}R$．

11.9 如果 $S = \{s_1, \cdots, s_n\}$ 是交换环 R 的有限非空子集，证明 $S^{-1}R \cong \{s\}^{-1}R$，其中 $s = s_1 \cdots s_n$．

提示：如果 s^{-1} 存在，则 $s^{-1}(s_1 \cdots \hat{s}_i \cdots s_n) = s_i^{-1}$ 存在．

11.10 证明 PID 的每个局部化也是 PID. 由此推出，如果 $\mathfrak{p}$ 是 PID R 中的素理想，则 $R_{\mathfrak{p}}$ 是 DVR.

11.11 如果 R 是布尔环且 $\mathfrak{m}$ 是 R 中的极大理想，证明 $R_{\mathfrak{m}}$ 是域．

11.12 设 S 是交换环 R 的子集，并设 I 和 J 都是 R 中的理想．

(i) 证明 $S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$．

(ⅱ) 证明 $S^{-1}(I:J)=(S^{-1}I:S^{-1}J)$.

11.13 如果一个整环 R 满足对一切 $a,b\in R$，或者 $a\mid b$，或者 $b\mid a$，则称 R 为**赋值环**.

(ⅰ) 证明每个 DVR 都是一个赋值环.

(ⅱ) 设 R 是整环且 $F=\mathrm{Frac}(R)$. 证明 R 是赋值环当且仅当对每个非零 $a\in F$，$a\in R$ 或 $a^{-1}\in R$.

11.14 (ⅰ) 证明赋值环中的每个有限生成理想都是主理想.

(ⅱ) 证明赋值环中的每个有限生成理想都是投射的.

11.15 如果一个阿贝尔群 Γ 是一个偏序集，其中只要 $a\leqslant a'$ 和 $b\leqslant b'$ 就有 $a+b\leqslant a'+b'$，则称 Γ 为**阿贝尔序群**；如果 Γ 的偏序是一个链，则称 Γ 为**阿贝尔全序群**. 域 k 上的一个**赋值**是指函数 $v:k^{\times}\to\Gamma$，其中 Γ 是阿贝尔全序群，满足

$$v(ab)=v(a)+v(b);$$
$$v(a+b)\geqslant\min\{v(a),v(b)\}.$$

(ⅰ) 如果 $a/b\in\mathbb{Q}$ 非零，记 $a=p^m a'$ 和 $b=p^n b'$，其中 $m,n\geqslant 0$ 和 $(a',p)=1=(b',p)$. 证明定义为 $v(a/b)=m-n$ 的 $v:\mathbb{Q}^{\times}\to\mathbb{Z}$ 是一个赋值.

(ⅱ) 如果 $v:k^{\times}\to\Gamma$ 是域 k 上的赋值，定义 $R=\{0\}\cup\{a\in k^{\times}:v(a)\geqslant 0\}$. 证明 R 是一个赋值环. (每个赋值环都是由它的分式域上的一个适当的赋值形成的. 此外，当阿贝尔全序群 Γ 同构于 $\mathbb{Z}$ 时，赋值环是离散的.)

(ⅲ) 证明 $a\in R$ 是单位当且仅当 $v(a)=0$.

(ⅳ) 证明每个赋值环都是一个 (未必诺特的) 局部环.

提示：证明 $\mathfrak{m}=\{a\in R:v(a)>0\}$ 是 R 中的唯一极大理想.

11.16 设 Γ 是阿贝尔全序群并设 k 是域. 定义 $k[\Gamma]$ 为群代数 (由几乎一切值都是 0 的一切函数 $f:\Gamma\to k$ 组成). 和通常一样，如果 $f(\gamma)=r_\gamma$，则记 f 为 $\sum_{\gamma\in\Gamma}r_\gamma\gamma$.

(ⅰ) 定义 $f=\sum_{\gamma\in\Gamma}r_\gamma\gamma$ 的次数为 α，如果 α 是满足 $r_\gamma\neq 0$ 最大的指标 γ. 证明 $k[\Gamma]$ 是赋值环，其中 $v(f)$ 是 f 的次数.

(ⅱ) 举出一个非诺特赋值环的例子.

11.17 如果一个交换环 R 的子集 S 是乘法封闭的，且 $ab\in S$ 蕴涵 $a\in S$ 和 $b\in S$，则称 S 为**饱和的**.

(ⅰ) 证明 R 中一切单位的集合 $U(R)$ 是 R 的饱和子集.

(ⅱ) 如果 $\mathcal{Z}(A)$ 是 R-模 A 上的一切零因子的集合，证明 $\mathcal{Z}(A)$ 的补是 R 的一个饱和子集.

(ⅲ) 如果 S 是交换环 R 的乘法封闭子集，证明存在包含 S 的唯一最小饱和子集 S'. (我们称 S' 为 S 的**饱和**). 证明 $(S')^{-1}R\cong S^{-1}R$.

(ⅳ) 证明一个乘法封闭子集是饱和的当且仅当它的补 $R-S$ 是素理想的并.

11.18 设 S 是交换环 R 的子集，并设 M 是有限生成 R-模. 证明 $S^{-1}M=\{0\}$ 当且仅当存在 $\sigma\in\overline{S}$ 使得 $\sigma M=\{0\}$.

11.19 设 S 是交换环 R 的子集，并设 A 是 R-模.

(ⅰ) 如果 A 是自由的，证明 $S^{-1}A$ 是自由 $(S^{-1}R)$-模.

(ⅱ) 如果 A 是有限生成的，证明 $S^{-1}A$ 是有限生成 $(S^{-1}R)$-模.

(ⅲ) 如果 A 是有限表现的，证明 $S^{-1}A$ 是有限表现 $(S^{-1}R)$-模.

11.20 如果 A 是投射的，证明 $S^{-1}A$ 是投射 $(S^{-1}R)$-模.

11.21 如果 $\mathfrak{p}$ 是交换环 R 中的素理想，又如果 A 是投射 R-模，证明 $A_\mathfrak{p}$ 是自由 $R_\mathfrak{p}$-模.

11.22 如果 B 是平坦 R-模，其中 R 是交换环，证明局部化 $S^{-1}B$ 是平坦 $(S^{-1}R)$-模.

提示：正合函子的复合是正合的.

11.23 (ⅰ) 举出一个阿贝尔群 B 的例子，满足 $\mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Q},B)\neq\{0\}$.

(ⅱ) 证明对 (ⅰ) 中的阿贝尔群 B，$\mathbb{Q}\otimes_{\mathbb{Z}}\mathrm{Ext}_{\mathbb{Z}}^{1}(\mathbb{Q},B)\neq\{0\}$.

(ⅲ) 证明：如果 R 是诺特的但 A 不是有限生成的，则命题 11.38 可能不成立.

11.24 设 R 是交换 k-代数，其中 k 是交换环，并设 M 是 k-模. 证明对一切 $n\geqslant 0$，

$$R\otimes_k \bigwedge^n(M)\cong \bigwedge^n(R\otimes_k M)$$

(当然，$\bigwedge^n(R\otimes_k M)$ 是指 R-模 $R\otimes_R M$ 的 n 次外幂). 由此推出，对 k 中的一切极大理想 $\mathfrak{m}$，

$$\left(\bigwedge^n(M)\right)_{\mathfrak{m}}\cong \bigwedge^n(M_{\mathfrak{m}}).$$

提示：证明 $R\otimes_k \bigwedge^n(M)$ 是关于交错 n-多重线性 R-函数的泛映射问题的解.

11.25 设 R 是交换诺特环. 如果 A 和 B 都是有限生成 R-模，证明对一切 n，$\mathrm{Tor}_n^R(A,B)$ 和 $\mathrm{Ext}_R^n(A,B)$ 都是有限生成 R-模.

11.2 戴得金环

毕达哥拉斯三元组是正整数的三元组 (a,b,c) 满足 $a^2+b^2=c^2$. 毕达哥拉斯三元组的例子是 $(3,4,5)$, $(5,12,13)$ 和 $(7,24,25)$，全体毕达哥拉斯三元组在习题 1.23 中进行了分类 (大约公元 100 年丢番图 (Diophantus) 对此有一个巧妙的几何证明). 费马证明不存在正整数 (a,b,c) 满足 $a^4+b^4=c^4$，并于 1637 年在丢番图的书的一个译本的空白处写着，他已经有了一个极好的证明：对任意 $n>2$，不存在正整数 (a,b,c) 满足 $a^n+b^n=c^n$. 费马的证明从未被发现，而他的注记 (那不过是他为自己所做的注释) 在他死后几年便闻名于世，当时他的儿子出版了他的著作. 费马还留下其他类似于这样的陈述，它们之中许多都是真的，有一些是错的，到 1800 年，他的陈述只有一个没有解决，被称为费马最后定理，这或许有点戏谑的意味. 它成为数论中突出的挑战之一，直到 1995 年，A. Wiles 才证明了费马最后定理.

每个正整数 $n>2$ 是 4 或某个奇素数 p 的倍数. 于是，如果不存在正整数 (a,b,c) 满足对某个奇素数 p 有 $a^p+b^p=c^p$，则费马最后定理成立 [如果 $n=pm$，则 $a^n+b^n=c^n$ 蕴涵 $(a^m)^p+(b^m)^p=(c^m)^p$]. 几个世纪以来，许多人企图证明它. 例如欧拉对 $n=3$ 发表了一个证明 (有漏洞，后来被纠正)，狄利克雷对 $n=5$ 发表了一个证明 (有漏洞，后来被纠正)，G. Lamé 对 $n=7$ 发表了一个正确的证明.

第一个重要进展 (不只是对个别的素数 p) 是在 19 世纪中叶得到的，归功于库默尔 (E. Kummer). 如果 $a^p+b^p=c^p$，其中 p 是奇素数，则研究的一个自然起点是恒等式

$$c^p=a^p+b^p=(a+b)(a+\zeta b)(a+\zeta^2 b)\cdots(a+\zeta^{p-1}b),$$

其中 $\zeta=\zeta_p$ 是 p 次单位原根. 库默尔证明，如果 $\mathbb{Z}[\zeta_p]$ 是 UFD，其中 $\mathbb{Z}[\zeta_p]=\{f(\zeta_p): f(x)\in\mathbb{Z}[x]\}$，则不存在正整数 a,b,c 满足 $a^p+b^p=c^p$. 另一方面，他证明存在素数 p，对于它 $\mathbb{Z}[\zeta_p]$ 不是 UFD. 为重建唯一分解，他发明了和 $\mathbb{Z}[\zeta_p]$ 有关的"理想数". 后来，戴得金重铸了库默尔的理想数成为我们现在理想的概念. 于是，费马最后定理成了近世代数和代数数论两者发展的催化剂. 戴得金环是类似 $\mathbb{Z}[\zeta_p]$ 环的相应推广，本节我们要对它进行研究.

11.2.1 整性

代数整数的概念是整元概念的特殊情形.

定义 *环扩张 R^*/R 是指一个包含 R 并把它作为子环的交换环 R^*. 假定 R^*/R 是环扩张，则元素 $a\in R^*$ 称为 R 上的*__整元__*，如果它是 $R[x]$ 中一个首一多项式的根. 一个环扩张 R^*/R 称为*__整扩__

张，如果每个 $a \in R^*$ 都是R上的整元．

例 11.40 **诺特正规化定理**常用来证明零点定理．它说，如果 k 是域且 A 是有限生成的 k-代数，则存在 A 中代数无关元素 $a_1,\cdots,a_n$ 使得 A 在 $k[a_1,\cdots,a_n]$ 上是整性的．见 Matsumura 所著的《Commutative Ring Theory》，262 页． ■

回忆一个复数如果是 $\mathbb{Z}[x]$ 中一个首一多项式的根，那么它是一个代数整数，因此代数整数是 $\mathbb{Z}$ 上的整元．读者应把下一引理和命题 7.24 相比较．

引理 11.41 如果 R^*/R 是环扩张，则在一个非零元素 $u \in R^*$ 上下列条件等价．

(i) u 是 R 上的整元．

(ii) 存在 R^* 的有限生成 R-子模 B 使得 $uB \subseteq B$．

(iii) 存在 R^* 的有限生成忠实 R-子模 B 使得 $uB \subseteq B$；即如果对某个 $d \in R$ 有 $dB = \{0\}$，则 $d = 0$.

证明 (i)⇒(ii)．如果 u 是 R 上的整元，存在首一多项式 $f(x) \in R[x]$ 使得 $f(u) = 0$；即存在 $r_i \in R$ 使得 $u^n = \sum_{i=0}^{n-1} r_i u^i$．定义 $B = \{1, u, u^2, \cdots, u^{n-1}\}$．显然 $uB \subseteq B$．

(ii) ⇒ (iii)．如果 $B = \langle b_1, \cdots, b_m \rangle$ 是 R^* 的有限生成 R-子模满足 $uB \subseteq B$，定义 $B' = \langle 1, b_1, \cdots, b_m \rangle$．现在 B'是有限生成的和忠实的（因为 $1 \in B'$），且 $uB' \subseteq B'$．

(iii) ⇒ (i)．假定存在 R^* 的忠实 R-子模，比如 $B = \langle b_1, \cdots, b_n \rangle$，使得 $uB \subseteq B$．则有 n 个方程的方程组 $ub_i = \sum_{j=1}^{n} p_{ij} b_j$，其中 $p_{ij} \in R$．如果 $P = [p_{ij}]$ 和 $X = (b_1, \cdots, b_n)^t$ 是 $n \times 1$ 列向量，则 $n \times n$ 方程组可以用矩阵记号重写为$(uI - P)X = 0$．现在根据系 9.161，$0 = (\mathrm{adj}(uI - P))(uI - P)X = dX$，其中 $d = \det(uI - P)$．因 $dX = 0$，对一切 i 有 $db_i = 0$，从而 $dB = \{0\}$．因为 B 是忠实的，所以 $d = 0$．另一方面，系 9.154 给出 $d = f(u)$，其中 $f(x) \in R[x]$ 是 n 次首一多项式；因此，u 是 R 上的整元． ■

整扩张是传递的．

命题 11.42 如果 $T \subseteq S \subseteq R$ 都是交换环，且 S 是 T 上的整扩张，R 是 S 上的整扩张，则 R 是 T 上的整扩张．

证明 如果 $r \in R$，存在等式 $r^n + s_{n-1} r^{n-1} + \cdots + r_0 = 0$，其中对一切 i，$s_i \in S$．根据引理 11.41，子环 $S' = T[s_{n-1}, \cdots, s_0]$ 是有限生成 T-模．但 r 是 S'上的整元，从而环 $S'[r]$ 是有限生成 S'-模．所以，$S'[r]$ 是有限生成 T-模，因此 r 是 T 上的整元． ■

命题 11.43 设 E/R 是环扩张．

(i) 如果 $u, v \in E$ 是 R 上的整元，则 uv 和 $u + v$ 都是 R 上的整元．

(ii) 由

$$\mathcal{O}_{E/R} = \{u \in E : u \text{ 是 } R \text{ 上的整元}\}$$

定义的交换环 $\mathcal{O}_{E/R}$ 是 E 的 R-子代数．

证明 (i) 因 u 和 v 都是 R 上的整元，引理11.41(ii)说存在 E 的R-子模 $B = \langle b_1, \cdots, b_n \rangle$ 和 $C = \langle c_1, \cdots, c_m \rangle$ 使得 $uB \subseteq B$ 和 $vC \subseteq C$；即对一切 i，$ub_i \in B$，而对一切 j，$vc_j \in C$．定义 BC 为由一切 $b_i c_j$ 生成的E 的 R-子模；当然，BC 是有限生成的．现在因为 $uvb_i c_j = (ub_i)(vc_j)$ 是 $b_k c_\ell s$ 的 R-线性组合，所以 $uvBC \subseteq BC$，因此 uv 是 R 上的整元．类似地，因为 $(u + v)b_i c_j = (ub_i)c_j + (vc_j)b_i \in BC$，$u + v$ 是 R 上的整元．

（ⅱ）由（ⅰ）可知 $\mathcal{O}_{E/R}$ 在乘法和加法下是封闭的．现在，如果 $r\in R$，则 r 是 $x-r$ 的根，因此 $R\subseteq\mathcal{O}_E$．由此 $1\in\mathcal{O}_{E/R}$ 且 $\mathcal{O}_{E/R}$ 是 E 的 R-子代数．■

这里有命题 11.43（ⅰ）对整环 E 的第二个证明，用到了张量积和线性代数．设 $f(x)\in R[x]$ 是 u 的极小多项式，A 是 $f(x)$ 的伴随矩阵，并设 y 是特征向量［在 Frac(E) 的代数闭包上］：$Ay=uy$. 设 $g(x)$ 是 v 的极小多项式，设 B 是 $g(x)$ 的伴随矩阵，并设 $Bz=vz$．现在

$$(A\otimes B)(y\otimes z)=Ay\otimes Bz=uy\otimes vz=uv(y\otimes z).$$

所以，uv 是 $A\otimes B$ 的一个特征值；即 uv 是首一多项式 $\det(xI-A\otimes B)$ 的根，因为 A 和 B 的一切元素都在 R 中，因此 $\det(XI-A\otimes B)$ 在 $R[x]$ 中．所以，uv 是 R 上的整元．类似地，等式

$$(A\otimes I+I\otimes B)(y\otimes z)=Ay\otimes z+y\otimes Bz=(u+v)y\otimes z$$

表明 $u+v$ 是 R 上的整元．■

定义　设 E/R 是环扩张．由 R 上的一切整元组成的 E 的 R-子代数 $\mathcal{O}_{E/R}$ 叫做 R 在 E 中的**整闭包**．如果 $\mathcal{O}_{E/R}=R$，则称 R 在 E 中是**整闭的**．如果 R 是整环且 R 在 $F=\mathrm{Frac}(R)$ 中是整闭的，即 $\mathcal{O}_{F/R}=R$，则称 R 为**整闭的**．

于是，R 是整闭的如果 $\alpha\in\mathrm{Frac}(R)$ 且 α 是 R 上的整元，则 $\alpha\in R$.

例 11.44　如果有理数 a 是 $\mathbb{Z}[x]$ 中的一个首一多项式的根，则定理 3.43 表明 $a\in\mathbb{Z}$，因此环 $\mathrm{O}_{\mathbb{Q}/\mathbb{Z}}=\mathbb{Z}$，从而 $\mathbb{Z}$ 是整闭的．■

命题 11.45　每个 UFD R 都是整闭的．特别地，每个 PID 都是整闭的．

证明　设 $F=\mathrm{Frac}(R)$，并假设 $u\in F$ 是 R 上的整元．于是，有等式

$$u^n+r_{n-1}u^{n-1}+\cdots+r_1u+r_0=0,$$

其中 $r_i\in R$. 我们可以记 $u=b/c$，其中 $b,c\in R$ 且 $(b,c)=1$（因为 R 是 UFD，所以 gcd 存在，从而每个分式可以写作既约形式）．代入并通分，

$$b^n+r_{n-1}b^{n-1}c+\cdots+r_1bc^{n-1}+r_0c^n=0.$$

因此，$b^n=-c(r_{n-1}b^{n-1}+\cdots+r_1bc^{n-2}+r_0c^{n-1})$，从而在 R 中 $c\mid b^n$．但 $(b,c)=1$ 蕴涵 $(b^n,c)=1$，因此 c 必是 R 中的单位；即 $c^{-1}\in R$. 所以，$u=b/c=bc^{-1}\in R$，从而 R 是整闭的．■

我们现在明白了例 6.21. 如果 k 是域，由一切没有线性项的多项式 $f(x)\in k[x]$ 组成的 $k[x]$ 的子环 R 不是 UFD，这是因为它不是整闭的．因为 $x=x^3/x^2\in\mathrm{Frac}(R)$，从而容易验证 $\mathrm{Frac}(R)=k(x)$．但 $x\in k(x)$ 是首一多项式 $t^2-x^2\in R[t]$ 的根，而 $x\notin R$.

定义　**代数数域**是指 $\mathbb{Q}$ 的一个有限域扩张．如果 E 是一个代数数域，则通常把 $\mathcal{O}_{E/\mathbb{Z}}$ 记为 $\mathcal{O}_E$，并称之为 E 中的**整数环**．

由于整数这个名词的新用法，代数数论中常把 $\mathbb{Z}$ 叫做**有理整数环**．

命题 11.46　设 E 是代数数域并设 $\mathcal{O}_E$ 是它的整数环．

（ⅰ）如果 $\alpha\in E$，存在非零整数 m 使得 $m\alpha\in\mathcal{O}_E$.

（ⅱ）$\mathrm{Frac}(\mathcal{O}_E)=E$.

（ⅲ）$\mathcal{O}_E$ 是整闭的．

证明　（ⅰ）如果 $\alpha\in E$，则存在首一多项式 $f(x)\in\mathbb{Q}[x]$ 使得 $f(\alpha)=0$．通分得整数 m 使得

$$m\alpha^n+c_{n-1}\alpha^{n-1}+c_{n-2}\alpha^{n-2}+\cdots+c_1\alpha+c_0=0,$$

其中一切 $c_i\in\mathbb{Z}$. 乘以 m^{n-1} 得

$$(m\alpha)^n+c_{n-1}(m\alpha)^{n-1}+mc_{n-2}(m\alpha)^{n-2}+\cdots+c_1m^{n-2}(m\alpha)+m^{n-1}c_0=0.$$

于是，$m\alpha \in \mathcal{O}_E$．

（ⅱ）只需证明如果 $\alpha \in E$，则存在 $a,b \in \mathcal{O}_E$ 使得 $\alpha = a/b$．但根据（ⅰ），$m\alpha \in \mathcal{O}_E$，$m \in \mathbb{Z} \subseteq \mathcal{O}_E$，从而 $\alpha = (m\alpha)/m$．

（ⅲ）假设 $\alpha \in \mathrm{Frac}(\mathcal{O}_E) = E$ 是 $\mathcal{O}_E$ 上的整元．根据命题 11.42，即整扩张的传递性，α 是 $\mathbb{Z}$ 上的整元．但这意味着 $\alpha \in \mathcal{O}_E$，根据定义 $\mathcal{O}_E$ 是 E 中在 $\mathbb{Z}$ 上为整元的那些元素的集合．所以，$\mathcal{O}_E$ 是整闭的． ■

例 11.47 在命题 11.76 中将看到，如果 $E = \mathbb{Q}(i)$，则 $\mathcal{O}_E = \mathbb{Z}[i]$，它是高斯整数．现在因为 $\mathbb{Z}[i]$ 是欧几里得环，所以它是 PID，因此也是 UFD. 这个例子的一个推广，即用一个代数数域 E 替换 $\mathbb{Q}(i)$ 比较深奥．$\mathcal{O}_E$ 是整闭的仍然为真，但 $\mathcal{O}_E$ 的元素是 α 的 $\mathbb{Z}$-线性组合可能不真．此外，环 $\mathcal{O}_E$ 可能不是 UFD. 本节末尾将研究整数环． ■

给定环扩张 R^*/R，R^* 中的理想和 R 中的理想有什么关系？

定义 设 R^*/R 是环扩张．如果 I 是 R 中的理想，定义它的**扩张** I^e 为 R^*I，它是由 I 生成的 R^* 中的理想．如果 I^* 是 R^* 中的理想，定义它的**收缩** $I^{*c} = R \cap I^*$．

注 这个定义可以推广．设 $h: R \to R^*$ 是环同态，其中 R 和 R^* 是任意两个交换环．定义 R 中一个理想 I 的扩张为由 $h(I)$ 生成的 R^* 中的理想；定义 R^* 中一个理想 I^* 的收缩为 $h^{-1}(I^*)$．如果 R^*/R 是环扩张，则取 $h: R \to R^*$ 为包含映射就得到上面的定义．另一个有趣的例子是局部化映射 $h: R \to S^{-1}R$．

例 11.48 （ⅰ）一般地，收缩函数 $c: \mathrm{Spec}(R^*) \to \mathrm{Spec}(R)$ 既不是单射也不是满射．例如，$c: \mathrm{Spec}(\mathbb{Q}) \to \mathrm{Spec}(\mathbb{Z})$ 不是满射，而 $c: \mathrm{Spec}(\mathbb{Q}[x]) \to \mathrm{Spec}(\mathbb{Q})$ 不是单射．

（ⅱ）易知，如果 R^*/R 是环扩张且 $\mathfrak{p}^*$ 是 R^* 中的素理想，则它的收缩 $\mathfrak{p}^* \cap R$ 也是素理想．如果 $a,b \in R$ 和 $ab \in \mathfrak{p}^* \cap R \subseteq \mathfrak{p}^*$，则 $\mathfrak{p}^*$ 是素理想给出 $a \in \mathfrak{p}^*$ 或 $b \in \mathfrak{p}^*$；因 $a,b \in R$，或者 $a \in \mathfrak{p}^* \cap R$，或者 $b \in \mathfrak{p}^* \cap R$．于是，收缩定义了一个函数 $c: \mathrm{Spec}(R^*) \to \mathrm{Spec}(R)$．

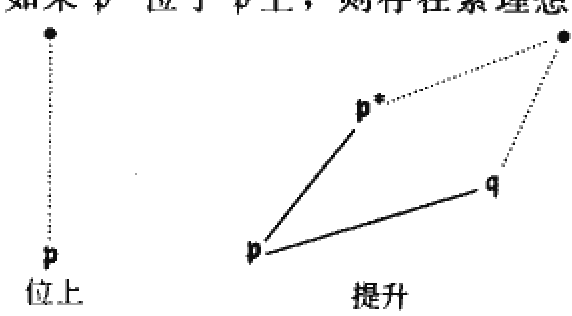
（ⅲ）极大理想的收缩虽然必定是素理想，但未必是极大的．例如，如果 R^* 是域，则 $\{0\}^*$ 是 R^* 中的极大理想，但如果 R 不是域，则 $\{0\}^*$ 的收缩，即 $\{0\}$ 就不是 R 中的极大理想． ■

例 11.49 （ⅰ）令 $\mathcal{I}(R)$ 表示一个交换环 R 中一切理想的族，扩张定义了一个函数 $e: \mathcal{I}(R) \to \mathcal{I}(R^*)$；一般来说，它既不是单射也不是满射．如果 R^* 是域而 R 不是域，则 $e: \mathcal{I}(R) \to \mathcal{I}(R^*)$ 不是单射；如果 R 是域而 R^* 不是域，则 $e: \mathcal{I}(R) \to \mathcal{I}(R^*)$ 不是满射．

（ⅱ）如果 R^*/R 是环扩张和 $\mathfrak{p}$ 是 R 中的素理想，则它的扩张 $R^*\mathfrak{p}$ 未必是素理想．首先，如果 $(a) = Ra$ 是 R 中的主理想，则它的扩张是由 a 生成的 R^* 中的主理想 R^*a．现在设 $R = \mathbb{R}[x]$ 和 $R^* = \mathbb{C}[x]$．因为 x^2+1 在 $\mathbb{R}[x]$ 中是不可约的，所以 (x^2+1) 是素理想，但它的扩张不是素理想，因为 x^2+1 在 $\mathbb{C}[x]$ 中可因式分解． ■

扩张和收缩有多种初等性质，诸如 $I^{*ce} \subseteq I^*$ 和 $I^{ce} \supseteq I$，它们收集在习题 11.28 中．

在环扩张 R^*/R 上是否有一个合理的条件可以给出 R 中的素理想和 R^* 中的素理想之间的好的关系？这个问题由 I. S. Cohen 和 A. Seidenberg 提出并给出了答案．我们说一个环扩张 R^*/R 满足**位上**，如果对 R 中的每个素理想 $\mathfrak{p}$ 存在 R^* 中的素理想 $\mathfrak{p}^*$ 使得 $\mathfrak{p}^* \cap R = \mathfrak{p}$．我们说 R^*/R 满足**提升**如果 $\mathfrak{p} \subseteq \mathfrak{q}$ 都是 R 中的素理想，且如果 $\mathfrak{p}^*$ 位于 $\mathfrak{p}$ 上，则存在素理想 $\mathfrak{q}^* \supseteq \mathfrak{p}^*$ 位于 $\mathfrak{q}$ 上．



我们要证明在整扩张中，扩张和收缩有良好的性态．

引理 11.50 设 R^* 是 R 的整扩张．

（ⅰ）如果 $\mathfrak{p}$ 是 R 中的素理想和 $\mathfrak{p}^*$ 位于 $\mathfrak{p}$ 上，则 $R^*/\mathfrak{p}^*$ 是 $R/\mathfrak{p}$ 的整扩张．

（ⅱ）设 S 是 R 的子集，则 $S^{-1}R^*$ 在 $S^{-1}R$ 上是整的．

证明 （ⅰ）首先，第二同构定理允许我们把 $R/\mathfrak{p}$ 看作 $R^*/\mathfrak{p}^*$ 的子环：

$$R/\mathfrak{p} = R/(\mathfrak{p}^* \cap R) \cong (R+\mathfrak{p}^*)/\mathfrak{p}^* \subseteq R^*/\mathfrak{p}^*.$$

$R^*/\mathfrak{p}^*$ 中的每个元素有 $\alpha+\mathfrak{p}^*$ 的形式，其中 $\alpha \in R^*$．因 R^* 是 R 的整扩张，有等式

$$\alpha^n + r_{n-1}\alpha^{n-1} + \cdots + r_0 = 0,$$

其中 $r_i \in R$．现在把这个等式 mod $\mathfrak{p}^*$ 可知 $\alpha+\mathfrak{p}^*$ 是 $R/\mathfrak{p}$ 上的整元．

（ⅱ）如果 $\alpha^* \in S^{-1}R^*$，则 $\alpha^* = \alpha/\sigma$，其中 $\alpha \in R^*$ 和 $\sigma \in \overline{S}$．因 R^* 是 R 的整扩张，有等式 $\alpha^n + r_{n-1}\alpha^{n-1} + \cdots + r_0 = 0$，其中 $r_i \in R$．在 $S^{-1}R^*$ 中乘以 $1/\sigma^n$ 得

$$(\alpha/\sigma)^n + (r_{n-1}/\sigma)(\alpha/\sigma)^{n-1} + \cdots + r_0/\sigma^n = 0,$$

由此证明 α/σ 是 $S^{-1}R$ 上的整元． ■

当 R^*/R 是环扩张且 R 是域时，R^* 中的每个真理想收缩为 R 中的 $\{0\}$．下一命题在 R^* 是 R 的整扩张时排除这种坍塌．

命题 11.51 设 R^*/R 是整环的环扩张，且 R^* 是 R 的整扩张．则 R^* 是域当且仅当 R 是域．

证明 假定 R^* 是域．如果 $u \in R$ 非零，则 $u^{-1} \in R^*$，从而 u^{-1} 是 R 上的整元．所以有等式 $(u^{-1})^n + r_{n-1}(u^{-1})^{n-1} + \cdots + r_0 = 0$，其中 $r_i \in R$．乘以 u^{n-1} 得 $u^{-1} = -(r_{n-1} + \cdots + r_0 u^{n-1})$．所以，$u^{-1} \in R$，因此 R 是域．

反之，假定 R 是域．如果 $\alpha \in R^*$ 非零，则有首一多项式 $f(x) \in R[x]$ 使得 $f(\alpha)=0$．于是，α 是 R 上的代数元素，因此可以假定 $f(x) = \mathrm{irr}(\alpha, R)$；即 $f(x)$ 是不可约的．如果 $f(x) = \sum_{i=0}^{n} r_i x^i$，则

$$\alpha(\alpha^{n-1} + r_{n-1}\alpha^{n-1} + \cdots + r_1) = -r_0.$$

$f(x)$ 的不可约性给出 $r_0 \neq 0$，从而 α^{-1} 在 R^* 中．所以 R^* 是域． ■

系 11.52 设 R^*/R 是整扩张．如果 $\mathfrak{p}$ 是 R 中的素理想且 $\mathfrak{p}^*$ 是位于 $\mathfrak{p}$ 上的素理想，则 $\mathfrak{p}$ 是极大理想当且仅当 $\mathfrak{p}^*$ 是极大理想．

证明 根据引理11.50（ⅰ），整环 $R^*/\mathfrak{p}^*$ 是整环 $R/\mathfrak{p}$ 上的整扩张．但现在命题 11.51 说 $R^*/\mathfrak{p}^*$ 是域当且仅当 $R/\mathfrak{p}$ 是域；即 $\mathfrak{p}^*$ 是 R^* 中的极大理想当且仅当 $\mathfrak{p}$ 是 R 中的极大理想． ■

系 11.53 如果 E 是代数数域，则 $\mathcal{O}_E$ 中的每个非零素理想都是极大理想．

证明 设 $\mathfrak{p}$ 是 $\mathcal{O}_E$ 中的非零素理想．如果 $\mathfrak{p} \cap \mathbb{Z} \neq \{0\}$，则根据例 11.48（ⅰ），存在素理想 p 使得 $\mathfrak{p} \cap \mathbb{Z} = (p)$．但 (p) 是$\mathbb{Z}$中的极大理想，因此，根据系 11.52，$\mathfrak{p}$ 是极大理想．剩下要证明 $\mathfrak{p} \cap \mathbb{Z} \neq \{0\}$．设 $\alpha \in \mathfrak{p}$ 是非零元素．因 α 是$\mathbb{Z}$上的整元，有等式

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0,$$

其中对一切 i，$c_i \in \mathbb{Z}$．如果在这种等式中选取一个 n 极小的等式，则 $c_0 \neq 0$．因 $\alpha \neq \mathfrak{p}$，有 $c_0 = -\alpha(\alpha^{n-1} + c_{n-1}\alpha^{n-2} + \cdots + c_1) \in \mathfrak{p} \cap \mathbb{Z}$，因此 $\mathfrak{p} \cap \mathbb{Z}$ 非零． ■

系 11.54　设 R^* 在 R 上是整的，$\mathfrak{p}$ 是 R 中的素理想，并设 $\mathfrak{p}^*$ 和 $\mathfrak{q}^*$ 是 R^* 中位于 $\mathfrak{p}$ 上的素理想．如果 $\mathfrak{p}^* \subseteq \mathfrak{q}^*$，则 $\mathfrak{p}^* = \mathfrak{q}^*$．

证明　引理 11.50（ⅱ）和系 11.18（ⅲ）表明局限在 $\mathfrak{p}$ 上假设仍然成立；即 $R_{\mathfrak{p}}^*$ 是 $R_{\mathfrak{p}}$ 的整扩张和 $\mathfrak{p}^* R_{\mathfrak{p}}^* \subseteq \mathfrak{q}^* R_{\mathfrak{p}}^*$ 都是素理想．因此，把 R^* 和 R 换成它们的局部化，可以假定 R^* 和 R 都是局部环且 $\mathfrak{p}$ 是 R 中的极大理想（根据命题 11.21）．但系 11.52 说 $\mathfrak{p}$ 的极大性迫使 $\mathfrak{p}^*$ 有极大性．因 $\mathfrak{p}^* \subseteq \mathfrak{q}^*$，所以 $\mathfrak{p}^* = \mathfrak{q}^*$．■

下面是 Cohen 和 Seidenberg 的定理．

定理 11.55（位上）　设 R^*/R 是环扩张且 R^* 是 R 的整扩张．如果 $\mathfrak{p}$ 是 R 中的素理想，则存在 R^* 中的素理想 $\mathfrak{p}^*$ 位于 $\mathfrak{p}$ 上；即 $\mathfrak{p}^* \cap R = \mathfrak{p}$．

证明　有交换图

$$\begin{array}{ccc} R & \xrightarrow{i} & R^*, \\ {\scriptstyle h}\downarrow & & \downarrow{\scriptstyle h^*} \\ R_{\mathfrak{p}} & \xrightarrow[j]{} & S^{-1}R^* \end{array}$$

其中 h 和 h^* 都是局部化映射，i 和 j 都是包含映射．如果 $S = R - \mathfrak{p}$，则 $S^{-1}R^*$ 是 $R_{\mathfrak{p}}$ 的扩张（因局部化是正合函子，R 包含在 R^* 中蕴涵 $R_{\mathfrak{p}}$ 包含在 $S^{-1}R^*$ 中）；根据引理 11.50，$S^{-1}R^*$ 是 $R_{\mathfrak{p}}$ 的整扩张．选取 $S^{-1}R^*$ 中的极大理想 $\mathfrak{m}^*$．根据系 11.52，$\mathfrak{m}^* \cap R_{\mathfrak{p}}$ 是 $R_{\mathfrak{p}}$ 中的极大理想．但 $R_{\mathfrak{p}}$ 是有唯一极大理想 $\mathfrak{p}R_{\mathfrak{p}}$ 的局部环，因此 $\mathfrak{m}^* \cap R_{\mathfrak{p}} = \mathfrak{p}R_{\mathfrak{p}}$．因素理想的逆象（在任意环映射下）也是素理想，理想 $\mathfrak{p}^* = (h^*)^{-1}(\mathfrak{m}^*)$ 是 R^* 中的素理想．现在

$$(h^* i)^{-1}(\mathfrak{m}^*) = i^{-1}(h^*)^{-1}(\mathfrak{m}^*) = i^{-1}(\mathfrak{p}^*) = \mathfrak{p}^* \cap R,$$

而

$$(jh)^{-1}(\mathfrak{m}^*) = h^{-1}j^{-1}(\mathfrak{m}^*) = h^{-1}(\mathfrak{m}^* \cap R_{\mathfrak{p}}) = h^{-1}(\mathfrak{p}R_{\mathfrak{p}}) = \mathfrak{p}.$$

所以，$\mathfrak{p}^*$ 是位于 $\mathfrak{p}$ 上的素理想．■

定理 11.56（提升）　设 R^*/R 是环扩张且 R^* 是 R 的整扩张．如果 $\mathfrak{p} \subseteq \mathfrak{q}$ 是 R 中的素理想，$\mathfrak{p}^*$ 是 R^* 中位于 $\mathfrak{p}$ 上的素理想，则存在位于 $\mathfrak{q}$ 上的素理想 $\mathfrak{q}^*$ 满足 $\mathfrak{p}^* \subseteq \mathfrak{q}^*$．

证明　引理 11.50 说 $(R^*/\mathfrak{p}^*)(R/\mathfrak{p})$ 是整环扩张，其中 $R/\mathfrak{p}$ 作为 $(R+\mathfrak{p}^*)/\mathfrak{p}^*$ 嵌入 $R^*/\mathfrak{p}^*$．把 R^* 和 R 换成商环，可以假定 $\mathfrak{p}^*$ 和 $\mathfrak{p}$ 都是 $\{0\}$．现在从位上定理立刻可得这个定理．■

还有一个下降定理，但需要一个附加假设．

定理（下降）　设 R^*/R 是整扩张并假定 R 是整闭的．如果 $\mathfrak{p}_1 \supseteq \mathfrak{p}_2 \supseteq \cdots \supseteq \mathfrak{p}_n$ 是 R 中素理想的链，又如果 $\mathfrak{p}_1^* \supseteq \mathfrak{p}_2^* \supseteq \cdots \supseteq \mathfrak{p}_m^*$（其中 $m < n$）是 R^* 中素理想的链，且每个 $\mathfrak{p}_i^*$ 位于 $\mathfrak{p}_i$ 上，则 R^* 中的链能够扩张为 $\mathfrak{p}_1^* \supseteq \mathfrak{p}_2^* \supseteq \cdots \supseteq \mathfrak{p}_n^*$，且对一切 $i \leqslant n$，$\mathfrak{p}_i^*$ 位于 $\mathfrak{p}_i^*$ 上．

证明　见 Atiyah-Macdonald 所著的《Introduction to Commutative Algebra》，64 页．■

习题

11.26　如果 R 是整闭整环且 S 是 R 的不包含 0 的乘法封闭子集，证明 $S^{-1}R$ 也是整闭的．

11.27　证明每个赋值环是整闭的．

11.28　设 R^*/R 是环扩张．如果 I 是 R 中的理想，记它的扩张为 I^e；如果 I^* 是 R^* 中的理想，记它的收缩为 I^{*c}．证明下面的论断．

(i) e 和 c 都保持包含关系：如果 $I \subseteq J$，则 $I^e \subseteq J^e$；如果 $I^* \subseteq J^*$，则 $I^{*c} \subseteq J^{*c}$.

(ii) $I^{*ce} \subseteq I^*$ 和 $I^{ec} \supseteq I$.

(iii) $I^{*cec} = I^{*c}$ 和 $I^{ece} = I^e$.

(iv) $(I^* + J^*)^c \supseteq I^{*c} + J^{*c}$ 和 $(I+J)^e = I^e + J^e$.

(v) $(I^* \cap J^*)^c = I^{*c} \cap J^{*c}$ 和 $(I \cap J)^e \subseteq I^e \cap J^e$.

(vi) $(I^* J^*)^c \supseteq I^{*c} J^{*c}$ 和 $(IJ)^e = I^e J^e$.

(vii) $(\sqrt{I^*})^c = \sqrt{I^{*c}}$ 和 $(\sqrt{I})^e \subseteq \sqrt{I^e}$.

(viii) $(J^* : I^*)^c \subseteq (J^{*c} : I^{*c})$ 和 $(I : J)^e \subseteq (I^e : J^e)$.

11.29 如果$\mathbb{A}$ 是一切代数数的域，则 $\mathcal{O}_{\mathbb{A}}$ 是一切代数整数的环．证明

$$\mathcal{O}_{\mathbb{A}} \cap \mathbb{Q} = \mathbb{Z}.$$

由此推出，对每个代数数域 E，$\mathcal{O}_E \cap \mathbb{Q} = \mathbb{Z}$.

11.30 设 R^*/R 整环扩张．

(i) 如果 $a \in R$ 是 R^* 中的单位，证明 a 是 R 中的单位．

(ii) 证明 $J(R) = R \cap J(R^*)$，其中 $J(R)$ 是雅各布森根．

11.31 设 R^*/R 是整扩张．如果 $\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \cdots \subseteq \mathfrak{p}_n$ 是 R 中素理想的链，又如果 $\mathfrak{p}_1^* \subseteq \mathfrak{p}_2^* \subseteq \cdots \subseteq \mathfrak{p}_m^*$（其中 $m < n$）是 R^* 中素理想的链，且每个 $\mathfrak{p}_i^*$ 位于 $\mathfrak{p}_i$ 上，则 R^* 中的链可以扩张为 $\mathfrak{p}_1^* \subseteq \mathfrak{p}_2^* \subseteq \cdots \subseteq \mathfrak{p}_n^*$，且对一切 $i \leqslant n$，$\mathfrak{p}_i^*$ 位于 $\mathfrak{p}_i$ 上．（所以叫做提升定理就是因为 R^* 中理想的链是递增的，与之相比，在下降定理中，R^* 中理想的链是递减的．）

11.32 设 R^*/R 是整扩张．如果 R 中的每个非零素理想都是极大理想，证明 R^* 中的每个非零素理想也是极大理想．

提示：见系 11.53 的证明．

11.33 设 α 是 $\mathbb{Q}$ 上的代数元素，设 $E/\mathbb{Q}$ 是分裂域，并设 $G = \mathrm{Gal}(E/\mathbb{Q})$ 是伽罗瓦群．

(i) 证明：如果 α 是 $\mathbb{Z}$ 上的整元，则对一切 $\sigma \in G$，$\sigma(\alpha)$ 也是 $\mathbb{Z}$ 上的整元．

(ii) 证明 α 是代数整数当且仅当 $\mathrm{irr}(\alpha, \mathbb{Q}) \in \mathbb{Z}[x]$．把这个证明和系 6.29 的证明相比较．

(iii) 设 E 是代数数域，并设 $R \subseteq E$ 是整闭的．如果 $\alpha \in E$，证明 $\mathrm{irr}(\alpha, \mathrm{Frac}(R)) \in R[x]$.

提示：如果 $\hat{E}$ 是 $\mathrm{Frac}(R)$ 的包含 α 的伽罗瓦扩张，则 $G = \mathrm{Gal}(\hat{E}/\mathrm{Frac}(R))$ 可传递地作用在 α 的根上．

11.2.2 回到零点定理

在本小节中，我们要对任意代数闭域证明零点定理（回忆第 6 章中的证明中假定了 k 是不可数的）．这个结果有不同的证明，我们展示的证明由 O. Goldman 发现，Kaplansky 在他的《Commutative Rings》中作了详细解释．

定义 *如果对于环扩张 A/R 存在满射 R-代数映射 $\varphi: R[x_1, \cdots, x_n] \to A$，则称环扩张 A/R 是***有限生成的**．*如果 $\varphi(x_i) = a_i$，则我们记*

$$A = R[a_1, \cdots, a_n].$$

如果 I 是交换环 R 中的理想，则 R/I 中的幂零元素由$\sqrt{I}$的元素形成．我们现在准备给出克鲁尔（W. Krull）的一个定理，它刻画了交换环中的幂零元素，这将给予我们理想的根的信息．

引理 11.57 *设 R 是整环且 $F = \mathrm{Frac}(R)$．则 F/R 是有限生成的环扩张当且仅当 F/R 是单一生成的环扩张；即存在 $u \in R$ 使得 $F = R[u^{-1}]$（因此，局部化 $\{u\}^{-1}R$ 是域）.*

证明　充分性是显然的，因此只证明必要性．如果 $F=R[a_1/b_1,\cdots,a_n/b_n]$，定义 $u=\prod_i b_i$．我们断言 $F=R[u^{-1}]$．显然，$F\supseteq R[u^{-1}]$．关于反包含，注意 $a_i/b_i=a_i\hat{u}_i/u\in R[u^{-1}]$ 其中 $\hat{u}_i=b_1\cdots\hat{b}_i\cdots b_n$．■

定义　设 R 是整环且 $F=\mathrm{Frac}(R)$，如果 F/R 是有限生成环扩张，则称 R 为 **G-整环**．设 I 是交换环 R 中的理想，如果 R/I 是 G-整环，则称 I 为 **G-理想**．⊖

每个域都是一个 G-整环，因此交换环中的每个极大理想都是一个 G-理想．如果 I 是 G-理想，则 R/I 是 G-整环，因此是整环；所以每个 G-理想都是素理想．系 11.61 说 $\mathbb{Z}$ 不是 G-整环；由此，$\mathbb{Z}[x]$ 中的素理想 (x) 不是 G-理想．

命题 11.58　设 E/R 是环扩张，其中 E 和 R 都是整环．如果 E 是有限生成 R-代数且每个 $\alpha\in E$ 都是 R 上的代数元素（即 α 是 $R[x]$ 中一个非零多项式的根），则 R 是 G-整环当且仅当 E 是 G-整环．

证明　设 R 是 G-整环，因此有某个非零的 $u\in R$ 使得 $F=\mathrm{Frac}(R)=R[u^{-1}]$．因为 $u\in R\subseteq E$，所以 $E[u^{-1}]\subseteq\mathrm{Frac}(E)$．但 $E[u^{-1}]$ 是域 $F=R[u^{-1}]$ 上的代数整环，因此根据习题 11.35，$E[u^{-1}]$ 是域．因 $\mathrm{Frac}(E)$ 是包含 E 的最小域，有 $E[u^{-1}]=\mathrm{Frac}(E)$，从而 E 是 G-整环．

如果 E 是 G-整环，则存在 $v\in E$ 使得 $\mathrm{Frac}(E)=E[v^{-1}]$．根据假设，$E=R[b_1,\cdots,b_n]$，其中对一切 i，b_i 是 $F=\mathrm{Frac}(R)$ 上的代数元素．由于 $v\in E$，所以 v 是 R 上的代数元素，从而 v^{-1} 也是 R 上的代数元素．于是，存在首一多项式 $f_0(x),f_i(x)\in F[x]$ 使得 $f_0(v^{-1})=0$ 且对一切 $i\geqslant 1$，$f_i(b_i)=0$．通分后得到系数在 R 中的等式 $\beta_i f_i(b_i)=0$，其中 $i\geqslant 0$：

$$\beta_0(v^{-1})^{d_0}+\cdots=0$$
$$\beta_i b_i^{d_i}+\cdots=0.$$

定义 $R^*=R[\beta_0^{-1},\beta_1^{-1},\cdots,\beta_n^{-1}]$．因为每个 β_i 都是 R^* 中的单位，所以每个 b_i 都是 R^* 中的整元．显然，$E[v^{-1}]=R^*[v^{-1},b_1,\cdots,b_n]$．于是根据命题 11.43，域 $E[v^{-1}]$ 是 R^* 的整扩张（因 $E[v^{-1}]=R^*[v^{-1},b_1,\cdots,b_n]$，且出现的每个生成元都是 R^* 上的整元），根据命题 11.51，这迫使 R^* 是域．但因对一切 i，$\beta_i\in R$，从而 $R^*=R[\beta_0^{-1},\beta_1^{-1},\cdots,\beta_n^{-1}]\subseteq F$，因此 $R^*=F$．所以，$F=R[\beta_0^{-1},\beta_1^{-1},\cdots,\beta_n^{-1}]$ 是 R 的有限生成环扩张；即 R 是 G-整环．■

下一引理导出系 11.60，它是 G-整环的一个"内在的"刻画，只用 R 而不用 $\mathrm{Frac}(R)$ 来表达．

引理 11.59　设 R 是整环且 $F=\mathrm{Frac}(R)$．对非零元素 $u\in R$ 下列条件等价．

（i）u 在 R 的每个非零素理想中．

（ii）对 R 中的每个非零理想 I，存在整数 n 使得 $u^n\in I$．

（iii）R 是 G-整环；即 $F=R[u^{-1}]$．

证明　(i)⇒(ii)．假设存在非零理想 I 满足对一切 $n\geqslant 0$，$u^n\notin I$．如果 $S=\{u^n: n\geqslant 0\}$，则 $I\cap S=\varnothing$．根据佐恩引理，存在理想 $\mathfrak{p}$，它在满足 $I\subseteq\mathfrak{p}$ 和 $\mathfrak{p}\cap S=\varnothing$ 的一切理想中极大，根据习题 6.9，$\mathfrak{p}$ 是素理想．这与 u 在每个素理想中矛盾．

（ii）⇒（iii）．如果 $b\in R$ 且 $b\neq 0$，则根据假设，有某个 $n\geqslant 1$ 使得 $u^n\in(b)$．因此有某个 $r\in R$ 使得 $u^n=rb$，从而 $b^{-1}=ru^{-n}\in R[u^{-1}]$．所以 $F=R[u^{-1}]$．

⊖　G-理想是以 O. Goldman 的名字命名的．

(iii)⇒(i). 设 $\mathfrak{p}$ 是非零素理想. 如果 $b\in\mathfrak{p}$ 非零，则因 $F=R[u^{-1}]$, $b^{-1}=\sum_{i=0}^{n}r_iu^{-i}$，其中 $r_i\in R$. 所以 $u^n=b\left(\sum_i r_iu^{n-i}\right)$ 在 $\mathfrak{p}$ 中，这是因为 $b\in\mathfrak{p}$ 和 $\sum_i r_iu^{n-i}\in R$. 因 $\mathfrak{p}$ 是素理想，所以 $u\in\mathfrak{p}$. ■

系 11.60 *整环 R 是 G-整环当且仅当 $\bigcap_{\substack{\mathfrak{p}素\\ \mathfrak{p}\neq 0}}\mathfrak{p}\neq\{0\}$.*

证明 根据引理 11.59，R 是 G-整环当且仅当它有非零元素 u 在每个非零素理想之中. ■

系 11.61 *如果 R 是 PID，则 R 是 G-整环当且仅当 R 只有有限个素理想.*

证明 如果 R 是 G-整环，则 $I=\bigcap\mathfrak{p}\neq\{0\}$，其中 $\mathfrak{p}$ 遍历一切非零素理想. 如果 R 有无限个素理想，则有无限个不相伴的素元素；$p_1,p_2,\cdots$；即 (p_i) 是不同的素理想. 如果 $a\in I$，则对一切 i 有 $p_i|a$. 但 $a=q_1^{e_1}\cdots q_n^{e_n}$，其中 q_i 是不同的素元素，这与 PID R 中的因子分解唯一性矛盾.

反之，如果 R 只有有限个非零素理想，比如 $(p_1),\cdots,(p_m)$，则乘积 $p_1\cdots p_m$ 是非零元素且在 $\bigcap_i(p_i)$ 中. 所以，R 是 G-整环. ■

由此可知，每个 DVR 是 G-整环.

定义 如果 R 是交换环，则它的**诣零根**是指

$$\mathrm{nil}(R)=\{r\in R: r\text{ 是幂零的}\}.$$

我们注意 $\mathrm{nil}(R)$ 是理想. 如果 $r,s\in R$ 是幂零的，则有正整数 m 和 n 使得 $r^n=0=s^m$. 因此，

$$(r+s)^{m+n-1}=\sum_{i=0}^{m+n-1}\binom{m+n-1}{i}r^is^{m+n-1-i}.$$

如果 $i\geqslant n$，则 $r^i=0$，从而和式中第 i 项为 0；如果 $i<n$，则 $m+n-i-1\geqslant m$，$s^{m+n-1-i}=0$，此时和式中第 i 项也是 0. 于是 $(r+s)^{m+n-1}=0$ 且 $r+s$ 是幂零的. 最后，rs 是幂零的，这是因为 $(rs)^{mn}=r^{mn}s^{mn}=0$.

下一定理是克鲁尔的初始形式的改进，它把诣零根刻画为一切素理想的交.

定理 11.62 (克鲁尔) *如果 R 是交换环，则*

$$\mathrm{nil}(R)=\bigcap_{\mathfrak{p}=素理想}\mathfrak{p}=\bigcap_{\mathfrak{p}=G\text{-}理想}\mathfrak{p}.$$

注 如果 R 是整环，则 $\{0\}$ 是素理想，从而 $\mathrm{nil}(R)=\{0\}$（除此之外，整环中没有非零的幂零元素）. 一个交换环 R 中一切非零素理想的交可能比 $\mathrm{nil}(R)$ 大；例如，当 R 是 DVR 时就是如此.

证明 显然 $\mathrm{nil}(R)\subseteq\bigcap_{\mathfrak{p}=素理想}\mathfrak{p}\subseteq\bigcap_{\mathfrak{p}=G\text{-}理想}\mathfrak{p}$：幂零元素在每个素理想中；每个 G-理想都是素理想. 于是，只需证明 $\bigcap_{\mathfrak{p}=G\text{-}理想}\mathfrak{p}\subseteq\mathrm{nil}(R)$. 假设 $u\notin\mathrm{nil}(R)$. 由此对一切 $n\geqslant 1$，$u^n\neq 0$. 所以乘法封闭集 $S=\{u^n:n\geqslant 1\}$ 不包含 0. 根据佐恩引理，存在理想 $\mathfrak{q}$ 在满足 $\mathfrak{q}\cap S=\varnothing$ 的理想中极大（存在理想与 S 不相交需有 $0\notin S$）. 我们断言 $\mathfrak{q}$ 是一个 G-理想，由此可得 $u\notin\bigcap_{\mathfrak{p}=G\text{-}理想}\mathfrak{p}$. 现在根据习题 6.9，$\mathfrak{q}$ 是素理想，从而 $R/\mathfrak{q}$ 是整环. 假设在 $R/\mathfrak{q}$ 中有非零素理想 $\mathfrak{p}^*$ 不包含 $u+\mathfrak{q}$. 则存在 R 中的理想 $\mathfrak{p}\supsetneq\mathfrak{q}$ 使得 $\mathfrak{p}^*=\mathfrak{p}/\mathfrak{q}$（因为 $\mathfrak{p}^*\neq\{0\}$），与 $\mathfrak{q}$ 的极大性矛盾. 所以 $u+\mathfrak{q}$ 在 $R/\mathfrak{q}$ 中每个非零素理想之中. 根据系

11.60，$R/\mathfrak{q}$ 是 G-整环，从而 $\mathfrak{q}$ 是 G-理想． ■

下一个系容易从克鲁尔定理得到．

系 11.63 如果 I 是交换环 R 中的理想，则$\sqrt{I}$是一切包含 I 的 G-理想的交．

证明 根据定义，$\sqrt{I}=\{r\in R$：有某个 $n\geqslant 1$ 使得 $r^n\in I\}$．所以$\sqrt{I}/I=\mathrm{nil}(R/I)=\bigcap_{\mathfrak{p}^*=G\text{-理想}}\mathfrak{p}^*$．对每个 $\mathfrak{p}^*$，存在包含 I 的理想 $\mathfrak{p}$ 使得 $\mathfrak{p}^*=\mathfrak{p}/I$，从而$\sqrt{I}=\bigcap_{\mathfrak{p}/I=G\text{-理想}}\mathfrak{p}$. 最后，交中涉及的每个 $\mathfrak{p}$ 是 G-理想，这是因为 $R/\mathfrak{p}\cong(R/I)(\mathfrak{p}/I)=(R/I)/\mathfrak{p}^*$ 和 $(R/I)/\mathfrak{p}^*$ 是 G-整环． ■

我们现在关注 $R[x]$ 中的理想和 R 中的理想之间的关系．

命题 11.64 交换环 R 中的理想 I 是 G-理想当且仅当 I 是 $R[x]$ 中一个极大理想的收缩．

证明 如果 I 是 R 中的 G-理想，则 R/I 是 G-整环．因此，存在$u\in\mathrm{Frac}(R/I)$ 使得 $\mathrm{Frac}(R/I)=(R/I)[u^{-1}]$．设 $\varphi:(R/I)[x]\to(R/I)[u^{-1}]$ 是取 $x\mapsto u^{-1}$ 的 R-代数映射．因 φ 是到域 $(R/I)[u^{-1}]=\mathrm{Frac}(R/I)$ 上的满射，它的核 $\mathfrak{m}$ 是 $(R/I)[x]$ 中的极大理想．因 $\varphi|(R/I)$ 是单射，有 $\mathfrak{m}\cap(R/I)=\{0\}$．根据习题 6.2，存在 $R[x]$ 中必是极大的理想 $\mathfrak{m}'$使得 $\mathfrak{m}'/I=\mathfrak{m}$，从而 $\mathfrak{m}'\cap R=I$．

反之，假定 $\mathfrak{m}$ 是 $R[x]$ 中的极大理想满足 $\mathfrak{m}\cap R=I$．如果 $v:R[x]\to R[x]/\mathfrak{m}$ 是自然映射和 $u=v(x)$，则 $\mathrm{im}v=(R/I)[u]$ 是域．因此根据命题 11.58，R/I 是 G-整环，从而 I 是 G-理想． ■

记号 如果 I 是交换环 R 中的理想，又如果 $f(x)\in R[x]$，则把 $f(x)$ 的系数用 $\mathrm{mod}I$ 约化得 $(R/I)[x]$ 中的多项式，记这个多项式为 $\bar{f}(x)$；即如果 $f(x)=\sum_i a_ix^i$，其中 $a_i\in R$，则 $\bar{f}(x)=\sum_i(a_i+I)x^i$．

系 11.65 设 R 是交换环，并设 $\mathfrak{m}$ 是 $R[x]$ 中的极大理想．如果收缩 $\mathfrak{m}'=\mathfrak{m}\cap R$ 是 R 中的极大理想，则 $\mathfrak{m}=(\mathfrak{m}',f(x))$，其中 $f(x)\in R[x]$ 和 $\bar{f}(x)\in(R/\mathfrak{m}')[x]$ 是不可约的．如果 $R/\mathfrak{m}'$ 是代数闭的，则有某个 $a\in R$ 使得 $\mathfrak{m}=(\mathfrak{m}',x-a)$．

证明 首先，命题 11.64 说 $\mathfrak{m}'=\mathfrak{m}\cap R$ 是 R 中的 G-理想．考虑用 $\mathrm{mod}\mathfrak{m}'$ 约化系数的映射 $\varphi:R[x]\to(R/\mathfrak{m}')[x]$．因 φ 是满射，理想 $\varphi(\mathfrak{m})$ 是极大理想；即 $\varphi(\mathfrak{m})=(g(x))$，其中 $g(x)\in(R/\mathfrak{m}')[x]$ 是不可约的．所以，$\mathfrak{m}=(\mathfrak{m}',f(x))$，其中 $\varphi(f)=g$；即 $\bar{f}(x)=g(x)$． ■

极大理想恒为 G-理想，G-理想恒为素理想．下一定义附加一个条件使得 G-理想成为极大理想．根据命题 11.64，这将迫使 $R[x]$ 中极大理想的收缩是 R 中的极大理想．

定义 对于一个交换环 R，如果每个 G-理想都是极大理想，则称 R 为**雅各布森**[⊖]环．

例 11.66 (i) 每个域都是雅各布森环．

(ii) 根据系 11.61，一个 PID R 是 G-整环当且仅当它只有有限个素理想．这样的环不可能是雅各布森环，因为 $\{0\}$ 是 G-理想，但不是极大的 [$R/\{0\}\cong R$ 是 G-整环]．另一方面，如果 R 有无限个素理想，则 R 不是 G-整环且$\{0\}$不是 G-理想．现在 G-理想是非零素理想，它必是极大的．所以，PID 是雅各布森环当且仅当它有无限个素理想．

⊖ 一些作者把这种环叫做希尔伯特环．1951 年，克鲁尔和 O. Goldman 独立地用本小节中的方法发表了零点定理的证明．克鲁尔在它的论文中引入了雅各布森环这个术语．

(iii) 我们注意，如果 R 是雅各布森环，则任意商 $R^*=R/I$ 也是．如果 $\mathfrak{p}^*$ 是 R^* 中的 G－理想，则 $R^*/\mathfrak{p}^*$ 是 G－整环．现在有 R 中的某个理想 $\mathfrak{p}$ 使得 $\mathfrak{p}^*=\mathfrak{p}/I$ 和 $R/\mathfrak{p}\cong(R/I)/(\mathfrak{p}/I)=R^*/\mathfrak{p}^*$．于是 $\mathfrak{p}$ 是 R 中的 G－理想．因 R 是雅各布森环，所以 $\mathfrak{p}$ 是极大理想，且 $R/\mathfrak{p}\cong R^*/\mathfrak{p}^*$ 是域．所以 $\mathfrak{p}^*$ 是极大理想，从而 R^* 也是雅各布森环．

(iv) 根据系 11.63，交换环 R 中的每个根理想都是包含它的一切 G－理想的交．所以，如果 R 是雅各布森环，则每个根理想都是极大理想的交． ■

例 11.66(iv)引出下面的结果．

命题 11.67 *交换环 R 是雅各布森环当且仅当 R 中的每个素理想都是极大理想的交．*

证明 根据系 11.63，每个根理想，因此每个素理想是包含 I 的一切 G－理想的交．但在雅各布森环中，每个 G－理想都是极大理想．

反之，假定 R 中的每个素理想都是极大理想的交．我们让读者验证这个性质被商环继承．设 $\mathfrak{p}$ 是 R 中的 G－理想，从而 $R/\mathfrak{p}$ 是 G－整环．于是 $R/\mathfrak{p}$ 中存在 $u\neq 0$ 使得 $\mathrm{Frac}(R/\mathfrak{p})=(R/\mathfrak{p})[u^{-1}]$．根据引理 11.59，$u$ 在 $R/\mathfrak{p}$ 的每个非零素理想中，因此 u 在每个非零极大理想中．现在 $R/\mathfrak{p}$ 中的每个素理想都是极大理想的交，特别地，因 $R/\mathfrak{p}$ 是整环，存在极大理想 $\mathfrak{m}_\alpha$ 使得 $\{0\}=\bigcap_\alpha \mathfrak{m}_\alpha$．如果所有这些 $\mathfrak{m}_\alpha$ 都非零，则 $u\in\bigcap_\alpha \mathfrak{m}_\alpha=\{0\}$，这是一个矛盾．由此可知 $\{0\}$ 是极大理想．所以 $R/\mathfrak{p}$ 是域，G－理想 $\mathfrak{p}$ 是极大的，且 R 是雅各布森环． ■

系 11.68 *交换环 R 是雅各布森环当且仅当对每个理想 I，$J(R/I)=\mathrm{nil}(R/I)$．特别地，$J(R)=\mathrm{nil}(R)$．*

证明 设 R 是雅各布森环．如果 I 是 R 中的理想，则 $\sqrt{I}=\bigcap\mathfrak{m}$，其中 $\mathfrak{m}$ 是包含 I 的极大理想．现在 $J(R/I)$ 是 R/I 中一切极大理想的交；即 $J(R)=\bigcap(\mathfrak{m}/I)=(\bigcap\mathfrak{m})/I=\sqrt{I}/I$．另一方面，$\mathrm{nil}(R)$ 由 R/I 中的一切幂零元素组成．但 $0=(f+I)^n=f^n+I$ 成立当且仅当 $f^n\in I$；即 $f\in\sqrt{I}$．为证明逆命题，注意条件说 R 中的每个根理想是极大理想的交．特别地，每个素理想是极大理想的交，因此 R 是雅各布森环． ■

下一结果将给出许多雅各布森环的例子．

定理 11.69 *交换环 R 是雅各布森环当且仅当 $R[x]$ 是雅各布森环．*

证明 我们已知雅各布森环的每个商都是雅各布森环．因此，如果 $R[x]$ 是雅各布森环，则 $R\cong R[x]/(x)$ 也是雅各布森环．

反之，假设 R 是雅各布森环．如果 $\mathfrak{q}$ 是 $R[x]$ 中的 G－理想，则根据习题 11.36，可以假定 $\mathfrak{q}\cap R=\{0\}$．如果 $\nu: R[x]\to R[x]/\mathfrak{q}$ 是自然映射，则 $R[x]/\mathfrak{q}=R[u]$，其中 $u=\nu(x)$．现在 $R[u]$ 是 G－整环，这是因为 $\mathfrak{q}$ 是 G－理想；因此，如果 $K=\mathrm{Frac}(R[u])$，则存在 $v\in K$ 使得 $K=R[u][v^{-1}]$．如果 $\mathrm{Frac}(R)=F$，则

$$K=R[u][v^{-1}]\subseteq F[u][v^{-1}]\subseteq K,$$

因此 $F[u][v^{-1}]=K$；即 $F[u]$ 是 G－整环．但如果 u 是 F 上的超越元素，则 $F[x]\cong F[u]$ 有无限个素理想，因此，根据系 11.61，$F[u]$ 不是 G－整环．于是 u 是 F 上的代数元素，从而 u 是 R 上的代数元素．因 $R[u]$ 是 G－整环，命题 11.58 说 R 是 G－整环．现在 R 是雅各布森环，因此根据习题 11.34，R 是域．但如果 R 是域，则因为 u 是 R 上的代数元素，$R[u]$ 也是域．所以，$R[u]=R[x]/\mathfrak{q}$ 是域，从而 $\mathfrak{q}$ 是极大理想，$R[x]$ 是雅各布森环． ■

系 11.70 如果 k 是域，则 $k[x_1,\cdots,x_n]$ 是雅各布森环.

证明 对 $n\geqslant 1$ 用归纳法证明. 关于基础步，根据习题 11.40，$k[x]$ 是有无限个素理想的 PID，因此根据例 11.66(ii)，它是雅各布森环. 关于归纳步，归纳假设给出 $R=k[x_1,\cdots,x_{n-1}]$ 是雅各布森环，适用定理 11.69. ■

定理 11.71 如果 $\mathfrak{m}$ 是 $k[x_1,\cdots,x_n]$ 中的极大理想，其中 k 是代数闭域，则存在 $a_1,\cdots,a_n\in k$ 使得

$$\mathfrak{m}=(x_1-a_1,\cdots,x_n-a_n).$$

证明 对 $n\geqslant 1$ 用归纳法证明. 如果 $n=1$，则 $\mathfrak{m}=(p(x))$，其中 $p(x)\in k[x]$ 是不可约的. 因 k 是代数闭域，所以 $p(x)$ 是线性的. 关于归纳步，设 $R=k[x_1,\cdots,x_{n-1}]$. 系 11.70 说 R 是雅各布森环，因此根据命题 11.64，$\mathfrak{m}\cap R$ 是 R 中的 G-理想. 因 R 是雅各布森环，$\mathfrak{m}'=\mathfrak{m}\cap R$ 是极大理想. 现在应用系 11.65 得 $\mathfrak{m}=(\mathfrak{m}',f(x_n))$，其中 $f(x_n)\in R[x_n]$ 和 $\overline{f}(x_n)\in(R/\mathfrak{m}')[x_n]$ 是不可约的. 由于 k 是代数闭域且 $R/\mathfrak{m}'$ 是有限生成 k-代数，$R/\mathfrak{m}'\cong k$，从而可以假定 $f(x_n)$ 是线性的，即存在 $a_n\in k$ 使得 $f(x_n)=x_n-a_n$. 根据归纳假设，$\mathfrak{m}'=(x_1-a_1,\cdots,x_{n-1}-a_{n-1})$，其中 $a_1,\cdots,a_{n-1}\in k$，这就完成了证明. ■

我们用定理 11.71 证明定理 6.100，即弱零点定理. 回忆第 6 章中只对不可数代数闭域的特殊情形证明了零点定理.

定理 11.72 (弱零点定理) 如果 $f_1(X),\cdots,f_t(X)\in k[X]$，其中 k 是代数闭域，则 $I=(f_1,\cdots,f_t)$ 是 $k[X]$ 中的真理想当且仅当 $\mathrm{Var}(f_1,\cdots,f_t)\neq\varnothing$.

证明 如果 I 是真理想，则存在包含它的极大理想 $\mathfrak{m}$. 根据定理 6.100，存在 $a=(a_1,\cdots,a_n)\in k^n$ 使得 $\mathfrak{m}=(x_1-a_1,\cdots,x_n-a_n)$. 现在 $I\subseteq\mathfrak{m}$ 蕴涵 $\mathrm{Var}(\mathfrak{m})\subseteq\mathrm{Var}(I)$. 但 $a\in\mathrm{Var}(\mathfrak{m})$，因此 $\mathrm{Var}(I)\neq\varnothing$. ■

我们现在可以重复 C 上零点定理的证明（定理 6.102）来得到任意代数闭域上的零点定理. 然而下面的证明更容易.

定理 11.73 (零点定理) 设 k 是代数闭域. 如果 I 是 $k[x_1,\cdots,x_n]$ 中的理想，则 $\mathrm{Id}(\mathrm{Var}(I))=\sqrt{I}$.

证明 易知包含关系 $\mathrm{Id}(\mathrm{Var}(I))\supseteq\sqrt{I}$. 如果对一切 $a\in\mathrm{Var}(I)$，$f^n(a)=0$，则对一切 $a\in\mathrm{Var}(I)$，$f(a)=0$，这是因为 f 的值在域 k 中. 因此 $f\in\mathrm{Id}(\mathrm{Var}(I))$. 关于反包含，先注意根据系 11.70，$k[x_1,\cdots,x_n]$ 是雅各布森环；因此，例 11.66（iv）证明 $\sqrt{I}$ 是极大理想的交. 设 $g\in\mathrm{Id}(\mathrm{Var}(I))$，如果 $\mathfrak{m}$ 是包含 I 的极大理想，则 $\mathrm{Var}(\mathfrak{m})\subseteq\mathrm{Var}(I)$，从而 $\mathrm{Id}(\mathrm{Var}(I))\subseteq\mathrm{Id}(\mathrm{Var}(\mathfrak{m}))$. 但 $\mathrm{Id}(\mathrm{Var}(\mathfrak{m}))=\mathfrak{m}$; $\mathrm{Id}(\mathrm{Var}(I))\supseteq\sqrt{\mathfrak{m}}=\mathfrak{m}$，这是因为 $\mathfrak{m}$ 是极大理想，因此是素理想. 所以正如所要的，$g\in\bigcap\mathfrak{m}=\sqrt{I}$. ■

习题

11.34 证明交换环 R 是域当且仅当 R 是雅各布森环且是 G-整环.

11.35 设 E/R 是环扩张，其中 R 是域且 E 是整环.

(i) 设 $b\in E$ 是 R 上的代数元素，证明存在等式

$$b^n+r_{n-1}b^{n-1}+\cdots+r_1b+r_0=0.$$

其中对一切 i，$r_i\in R$ 和 $r_0\neq 0$.

(ii) 如果 $E=R[b_1,\cdots,b_m]$，其中 b_j 是 R 上的代数元素，证明 E 是域.

11.36 设 R 是雅各布森环，并假定对 $R[x]$ 中的每个 G-理想 $\mathfrak{q}$，$(R/\mathfrak{q}')[x]$ 是雅各布森环，其中 $\mathfrak{q}'=\mathfrak{q}\cap R$. 证明 $R[x]$ 是雅各布森环.

11.37 (ⅰ) 证明 $\mathfrak{m}=(x^2-y,y^2-2)$ 是 $\mathbb{Q}[x,y]$ 中的极大理想.

(ⅱ) 证明不存在 $f(x)\in\mathbb{Q}[x]$ 和 $g(y)\in\mathbb{Q}[y]$ 使得 $\mathfrak{m}=(f(x),g(y))$.

11.38 设 k 是域并设 $\mathfrak{m}$ 是 $k[x_1,\cdots,x_n]$ 中的极大理想. 证明

$$\mathfrak{m}=(f_1(x_1),f_2(x_1,x_2),\cdots,f_{n-1}(x_1,\cdots,x_{n-1}),f_n(x_1,\cdots,x_n)).$$

提示：用系 11.65.

11.39 证明：如果 R 是诺特环，则 $\operatorname{nil}(R)$ 是幂零理想.

11.40 如果 k 是域，证明 $k[x]$ 有无限个素理想.

11.2.3 代数整数

我们已经提到库默尔研究了环 $\mathbb{Z}[\zeta_p]$，其中 p 是奇素数且 ζ_p 是 p 次单位原根. 现在进一步研究代数数域 E 中的整数的环. 回忆定义

$$\mathcal{O}_E=\{\alpha\in E:\alpha\text{ 是}\mathbb{Z}\text{上的整元}\}.$$

我们从高斯引理的一个推论开始.

引理 11.74 设 E 是代数数域且 $[E:\mathbb{Q}]=n$，并设 $\alpha\in E$ 是代数整数. 则 $\operatorname{irr}(\alpha,\mathbb{Q})\in\mathbb{Z}[x]$ 且 $\deg(\operatorname{irr}(\alpha,\mathbb{Q}))\mid n$.

证明 根据系 6.29，$\operatorname{irr}(\alpha,\mathbb{Q})\in\mathbb{Z}[x]$，从而结果由命题 3.117(Ⅴ) 可得. ∎

定义 二次域是指一个代数数域 E 且 $[E:\mathbb{Q}]=2$.

命题 11.75 每个二次域 E 有 $E=\mathbb{Q}(\sqrt{d})$ 的形式，其中 d 是一个无平方因数的整数.

证明 我们知道 $E=\mathbb{Q}(\alpha)$，其中 α 是一个二次多项式的根，比如 $\alpha^2+b\alpha+c=0$，其中 $b,c\in\mathbb{Q}$. 如果 $D=b^2-4c$，则二次公式给出 $\alpha=-\frac{1}{2}b\pm\frac{1}{2}\sqrt{D}$，从而 $E=\mathbb{Q}(\alpha)=\mathbb{Q}(\sqrt{D})$. 把 D 写作既约形式：$D=U/V$，其中 $U,V\in\mathbb{Z}$ 且 $(U,V)=1$. 现在 $U=ur^2$ 和 $V=vs^2$，其中 u,v 无平方因数；因为 $(u,v)=1$，从而 uv 无平方因数. 因为 $\sqrt{u/v}=\sqrt{uv/v^2}=\sqrt{uv}/v$，所以 $\mathbb{Q}(\sqrt{D})=\mathbb{Q}(\sqrt{u/v})=\mathbb{Q}(\sqrt{uv})$. ∎

我们现在描述二次域中的整数.

命题 11.76 设 $E=\mathbb{Q}(\sqrt{d})$，其中 d 是无平方因数的整数（这蕴涵 $d\not\equiv 0\bmod 4$）.

(ⅰ) 如果 $d=2\bmod 4$ 或 $d=3\bmod 4$，则 $\mathcal{O}_E=\mathbb{Z}[\sqrt{d}]$.

(ⅱ) 如果 $d=1\bmod 4$，则 $\mathcal{O}_E$ 由一切 $\frac{1}{2}(u+v\sqrt{d})$ 组成，其中 u,v 是有相同奇偶性的有理整数.

证明 如果 $\alpha\in E=\mathbb{Q}(\sqrt{d})$，则存在 $a,b\in\mathbb{Q}$ 使得 $\alpha=a+b\sqrt{d}$. 我们先证明 $\alpha\in\mathcal{O}_E$ 当且仅当

$$2a\in\mathbb{Z}\text{ 和 }a^2-db^2\in\mathbb{Z}. \tag{3}$$

如果 $\alpha\in\mathcal{O}_E$，则引理 11.74 说 $p(x)=\operatorname{irr}(\alpha,\mathbb{Q})\in\mathbb{Z}[x]$ 是二次多项式. 现在 $\operatorname{Gal}(E/\mathbb{Q})=\langle\sigma\rangle$，其中 $\sigma:E\to E$ 把 $\sqrt{d}\mapsto-\sqrt{d}$；即

$$\sigma(\alpha)=a-b\sqrt{d}.$$

因 σ 置换 $p(x)$ 的根，$p(x)$ 的另一个根是 $\sigma(\alpha)$；即

$$p(x)=(x-\alpha)(x-\sigma(\alpha))=x^2-2ax+(a^2-db^2).$$

因为 $p(x)\in\mathbb{Z}[x]$，所以（3）式成立．

反之，如果（3）式成立，则 $\alpha\in\mathcal{O}_E$，这是因为 α 是 $\mathbb{Z}[x]$ 中首一多项式 $x^2-2ax+(a^2-db^2)$ 的根．

我们现在证明 $2b\in\mathbb{Z}$．(3) 式中的第二个等式乘以 4 得 $(2a)^2-d(2b)^2\in\mathbb{Z}$．因 $2a\in\mathbb{Z}$，我们有 $d(2b)^2\in\mathbb{Z}$．把 $2b$ 写作既约形式：$2b=m/n$，其中 $(m,n)=1$．现在 $dm^2/n^2\in\mathbb{Z}$，从而 $n^2\mid dm^2$．但 $(n^2,m^2)=1$ 迫使 $n^2\mid d$；由于 d 是无平方因数的，所以 $n=1$ 且 $2b=m/n\in\mathbb{Z}$．

我们已经证明了 $a=\frac{1}{2}u$ 和 $b=\frac{1}{2}v$，其中 $u,v\in\mathbb{Z}$．把它们代入(3)中的第二个等式得

$$u^2\equiv dv^2 \bmod 4. \tag{4}$$

注意，平方 mod4 不是和 0 同余就是和 1 同余．如果 $d\equiv 2\bmod 4$，则满足(4)式的唯一方式是 $u^2\equiv 0\bmod 4$ 和 $v^2\equiv 0\bmod 4$．于是 u 和 v 都必是偶数，从而 $\alpha=\frac{1}{2}u+\frac{1}{2}v\sqrt{d}\in\mathbb{Z}[\sqrt{d}]$．易知 $\mathbb{Z}[\sqrt{d}]\subseteq\mathcal{O}_E$，所以在这种情形下，$\mathcal{O}_E=\mathbb{Z}[\sqrt{d}]$．当 $d\equiv 3\bmod 4$ 时可进行类似的论证．然而，如果 $d\equiv 1\bmod 4$，则 $u^2\equiv v^2\bmod 4$，因此 v 是偶数当且仅当 u 是偶数；即 u,v 有相同的奇偶性．如果 u,v 都是偶数，则 $a,b\in\mathbb{Z}$ 和 $\alpha\in\mathcal{O}_E$．如果 u,v 都是奇数，则 $u^2\equiv 1\equiv v^2\bmod 4$，因为 $d\equiv 1\bmod 4$，从而 $u^2\equiv dv^2\bmod 4$．所以（3）式成立，因此 α 在 $\mathcal{O}_E$ 中． ■

如果 $E=\mathbb{Q}(\sqrt{d})$，其中 $d\in\mathbb{Z}$，则 $\mathbb{Z}[\sqrt{d}]\subseteq\mathcal{O}_E$，但现在可知这个包含可以是严格的．例如，$\frac{1}{2}(1+\sqrt{5})$ 是代数整数（它是 x^2-x-6 的根），所以，$\mathbb{Z}[\sqrt{5}]\subsetneq\mathcal{O}_E$，其中 $E=\mathbb{Q}(\sqrt{5})$．

下面关于线性代数的简短讨论使我们能够证明整数的环 $\mathcal{O}_E$ 是诺特环．

定义 设 E/k 是域扩张，其中 E 是有限维的．如果 $u\in E$，则由 $\Gamma_u: y\mapsto uy$ 给出的乘映射 $\Gamma_u: E\to E$ 是 k-映射．如果 $e_1,\cdots,e_n$ 是 E 的基，则 Γ_u 由元素在 k 中的矩阵 $A=[a_{ij}]$ 表示；即

$$\Gamma_\mu(e_i)=ue_i=\sum a_{ij}e_j.$$

定义**迹** $\mathrm{tr}(u)=\mathrm{tr}(\Gamma_u)$ 和**范数** $N(u)=\det(\Gamma_u)$．定义**迹形式** $t: E\times E\to R$ 为

$$t(u,v)=\mathrm{tr}(uv)=\mathrm{tr}(\Gamma_{uv}).$$

线性变换的特征多项式不依赖于 E/k 的基的选取，因此它的任何系数也是这样，从而迹和范数的定义不依赖于基的选取．如果 $u\in k$，则 Γ_u 关于 E/k 的任意一组基的矩阵是标量矩阵 uI．因此，

$$\text{如果 } u\in k,\quad \mathrm{tr}(u)=[E:k]u \quad \text{和} \quad N(u)=u^{[E:k]}.$$

易知 $\mathrm{tr}: E\to k$ 是线性函数且 $N: E^\times\to k^\times$ 是（乘性）同态．

验证迹形式是对称双线性形式留给读者作为一个平淡的练习．

例 11.77 如果 $E=\mathbb{Q}(\sqrt{d})$ 是二次域，则 $E/\mathbb{Q}$ 的一组基是 1，$\sqrt{d}$．如果 $u=a+b\sqrt{d}$，则 Γ_u 的矩阵是

$$\begin{bmatrix} a & bd \\ b & a \end{bmatrix},$$

因此

$$\mathrm{tr}(u)=2a \quad \text{和} \quad N(u)=a^2-db^2=u\bar{u}, \text{其中 } \bar{u}=a-b\sqrt{d}.$$

于是，迹和范数产生(3)式那样对二次域中的整数的描述．

我们现在证明 $u=a+b\sqrt{d}$ 是 $\mathcal{O}_E$ 中的单位当且仅当 $N(u)=\pm 1$．如果 u 是单位，则存在 $v\in\mathcal{O}_E$ 使得 $1=uv$．因此 $1=N(1)=N(uv)=N(u)N(v)$，从而 $N(u)$ 是 $\mathbb{Z}$ 中的单位；即 $N(u)=\pm 1$．反

之，如果 $N(u)=\pm 1$，则 $N(\bar{u})=N(u)=\pm 1$，其中 $\bar{u}=a-b\sqrt{d}$．所以 $N(u\bar{u})=1$．但 $u\bar{u}\in\mathbb{Q}$，因此 $1=N(u\bar{u})=(u\bar{u})^2$．所以 $u\bar{u}=\pm 1$，从而 u 是单位． ■

引理 11.78 设 E/k 是有限次数 n 的域扩张，并设 $u\in E$．如果 $u=u_1,\cdots,u_s$ 是 $\operatorname{irr}(u,k)$ 的带有重数根（在 E 的某个扩域中），即 $\operatorname{irr}(u,k)=\prod_{i=1}^{s}(x-u_i)$，则

$$\operatorname{tr}(u)=[E:k(u)]\sum_{i=1}^{s}u_i \quad 和 \quad N(u)=\Big(\prod_{i=1}^{s}u_i\Big)^{[E:k(u)]}.$$

注 当然，如果 u 在 k 上是可分的，则 $\operatorname{irr}(u,k)$ 没有重根，在公式中每个 u_i 恰好出现一次．

证明概要 $k(u)$ 在 k 上的一组基是 $1,u,u^2,\cdots,u^{s-1}$，$\Gamma_u\mid k(u)$ 关于这组基的矩阵 C_1 是 $\operatorname{irr}(u,k)$ 的伴随矩阵．如果 $1,v_2,\cdots,v_r$ 是 E 在 $k(u)$ 上的基，则表

$$1,u,\cdots,u^{s-1},v_1,v_1u,\cdots,v_1u^{s-1},\cdots,v_r,v_ru,\cdots,v_ru^{s-1}$$

是 E 在 k 上的基．子空间 $k(u)$ 和 $\langle v_j,v_ju,\cdots,v_ju^{s-1}\rangle$（其中 $j\geqslant 2$）的每一个都是 Γ_u-不变量，因此 Γ_u 的矩阵关于上面给出的 E 在 k 上的基是块的直和 $C_1\oplus\cdots\oplus C_r$．事实上，读者可以验证每个 C_j 都是 $\operatorname{irr}(u,k)$ 的伴随矩阵．现在迹和范数公式可以由 $\operatorname{tr}(C_1\oplus\cdots\oplus C_r)=\sum_j\operatorname{tr}(C_j)$ 和 $\det(C_1\oplus\cdots\oplus C_r)=\prod_j\det(C_j)$ 得到． ■

如果 E/k 是域扩张和 $u\in E$，则关于迹和范数的更确切的概念是

$$\operatorname{tr}_{E/k}(u) \quad 和 \quad N_{E/k}(u).$$

的确，在引理 11.78 的公式中呈现出对大域 E 的依赖性．

命题 11.79 设 R 是整环且 $F=\operatorname{Frac}(R)$，设 E/F 是次数 $[E:F]=n$ 有限的域扩张，并设 $u\in E$ 是 R 上的整元．如果 R 是整闭的，则

$$\operatorname{tr}(u)\in R \quad 和 \quad N(u)\in R.$$

证明 引理 11.78 中的公式把 $\operatorname{tr}(u)$ 和 $N(u)$ 表示成 $\operatorname{irr}(u,F)$ 的根 $u=u_1,\cdots,u_s$ 的初等对称函数．因 u 是 R 上的整元，习题 11.33（ⅲ）说 $\operatorname{irr}(u,F)\in R[x]$．所以 $\sum_i u_i$ 和 $\prod_i u_i$ 都在 R 中，因此 $\operatorname{tr}(u)$ 和 $N(u)$ 在 R 中． ■

在例 4.35 中，我们知道，如果 E/k 是有限可分扩张，则它的正规闭包 $\hat{E}$ 是 k 的伽罗瓦扩张．回忆伽罗瓦理论的基本定理（定理 4.43）如果 $G=\operatorname{Gal}(\hat{E}/k)$ 和 $H=\operatorname{Gal}(\hat{E}/E)$，则 $[G:H]=[E:k]$.

引理 11.80 设 E/k 是有有限次数 $n=[E:k]$ 的可分域扩张，并设 $\hat{E}$ 是 E 的正规闭包．记 $G=\operatorname{Gal}(\hat{E}/k)$ 和 $H=\operatorname{Gal}(\hat{E}/E)$，并设 T 是 H 在 G 中的一个陪集代表系；即存在不相交并 $G=\bigcup_{\sigma\in T}\sigma H$．

（ⅰ）对一切 $u\in E$，

$$\prod_{\sigma\in T}(x-\sigma(u))=\operatorname{irr}(u,k)^{[E:k(u)]}.$$

（ⅱ）对一切 $u\in E$，

$$\operatorname{tr}(u)=\sum_{\sigma\in T}\sigma(u) \quad 和 \quad N(u)=\prod_{\sigma\in T}\sigma(u).$$

证明 （ⅰ）记 $\prod_{\sigma\in T}(x-\sigma(u))$ 为 $h(x)$；当然，$h(x)\in\hat{E}[x]$.

我们断言由 $X=\{\sigma(u):\sigma\in T\}$ 定义的集合 X 满足对每个 $\tau\in G$ 有 $\tau(X)=X$．如果 $\sigma\in T$，则

因 T 是左陪集代表系，有某个 $\sigma' \in T$ 使得 $\tau\sigma \in \sigma' H$；因此有某个 $\eta \in H$ 使得 $\tau\sigma = \sigma'\eta$. 但因 $\eta \in H$，从而 $\tau\sigma(u) = \sigma'\eta(u) = \sigma'(u)$，且 H 的每个元素固定 E. 所以 $\tau\sigma(u) = \sigma'(u) \in X$. 于是由 $\sigma(u) \mapsto \tau\sigma(u)$ 定义的函数 φ_τ 是函数 $X \to X$. 事实上，因为 τ 是同构并因此 $\varphi_\tau \mid X$ 是单射，所以 φ_τ 是置换. 由此，$X = \{\sigma(u) : \sigma \in T\}$ 上的每个初等对称函数被每个 $\tau \in G$ 固定. 因 $\hat{E}/k$ 是伽罗瓦扩张，这些初等对称函数的每个值都在 k 中. 我们已经证明了 $h(x)$ 的一切系数都在 k 中，从而 $h(x) \in k[x]$. 现在比较 $h(x)$ 和 $\mathrm{irr}(u,k)$. 如果 $\sigma \in G$，则 σ 置换 $\mathrm{irr}(u,k)$ 的根，因此 $h(x)$ 的每个根 $\sigma(u)$ 也是 $\mathrm{irr}(u,k)$ 的根. 根据习题 3.86，有某个 $m \geqslant 1$ 使得

$$h(x) = \mathrm{irr}(u,k)^m,$$

因此剩下的只是计算 m. 现在

$$\deg(h) = m\deg(\mathrm{irr}(u,k)) = m[k(u) : k].$$

但 $\deg(h) = [G : H] = [E : k]$，从而 $m = [E : k]/[k(u) : k] = [E : k(u)]$.

（ⅱ）回忆早先的记号：$\mathrm{irr}(u,k) = \prod_{i=1}^{s}(x - u_i)$. 因

$$\prod_{\sigma \in T}(x - \sigma(u)) = \mathrm{irr}(u,k)^{[E:k(u)]} = \Big(\prod_{i=1}^{s}(x - u_i)\Big)^{[E:k(u)]},$$

它们的常数项相同，

$$\pm \prod_{\sigma \in T}\sigma(u) = \pm\Big(\prod_{i=1}^{s} u_i\Big)^{[E:k(u)]},$$

它们倒数第二项的系数相同，

$$-\sum_{\sigma \in T}\sigma(u) = -[E : k(u)]\sum_{i=1}^{s} u_i.$$

根据引理 11.78，$\mathrm{tr}(u) = [E : k(u)]\sum_{i=1}^{s} u_i$ 和 $N(u) = \Big(\prod_{i=1}^{s} u_i\Big)^{[E:k(u)]}$. 由此

$$\mathrm{tr}(u) = [E : k(u)]\sum_{i=1}^{s} u_i = \sum_{\sigma \in T}\sigma(u)$$

和

$$N(u) = \Big(\prod_{i=1}^{s} u_i\Big)^{[E:k(u)]} = \prod_{\sigma \in T}\sigma(u).$$ ■

定义 *设 E/k 是有限域扩张，设 $\hat{E}$ 是 E 的正规闭包，并设 T 是 $\mathrm{Gal}(\hat{E}/E)$ 在 $\mathrm{Gal}(\hat{E}/k)$ 中的一个左陪集代表系. 如果 $u \in E$，则元素 $\sigma(u)$（其中 $\sigma \in T$）叫做 u 的***共轭***.*

如果 E/k 是可分扩张，则 u 的共轭是 $\mathrm{irr}(u,k)$ 的根；在不可分的情形中，共轭可能多重出现.

系 11.81 *如果 E/k 是伽罗瓦扩张且 $G = \mathrm{Gal}(E/k)$，则*

$$\mathrm{tr}(u) = \sum_{\sigma \in G}\sigma(u) \quad 和 \quad N(u) = \prod_{\sigma \in G}\sigma(u).$$

证明 因 E/k 是伽罗瓦扩张，E 是它自己的正规闭包，从而 $\mathrm{Gal}(\hat{E}/E) = \mathrm{Gal}(E/E) = 1$，而 1 在 G 中的一个陪集代表系就是 G. ■

上面的系表明这里的范数和希尔伯特定理 4.90 的证明中出现的范数是一致的.

设 V 是域 k 上的向量空间，并设 $f : V \times V \to k$ 为双线性型. 如果 $e_1, \cdots, e_n$ 是 V 的基，则判别式定义为

$$D(e_1, \cdots, e_n) = \det([f(e_i, e_j)]).$$

回忆 f 非退化如果它关于一组基的判别式非零（由此，f 关于 V 的任意一组基的判别式也非零).

引理 11.82 如果 E/k 是有限可分[⊖]域扩张，则迹形式是非退化的.

证明 我们用引理 11.80（它用到可分性）计算判别式. 设$T=\{\sigma_1,\cdots,\sigma_n\}$是 $\mathrm{Gal}(\hat{E}/E)$ 在 $\mathrm{Gal}(\hat{E}/k)$ 中的一个陪集代表系，其中 $\hat{E}$ 是 E 的正规闭包.

$$\begin{aligned}D(e_1,\cdots,e_n)&=\det([t(e_i,e_j)])\\&=\det([\mathrm{tr}(e_ie_j)])\\&=\det\Big[\sum_\ell\sigma_\ell(e_ie_j)\Big]\qquad(\text{引理 }11.80)\\&=\det\Big(\Big[\sum_\ell\sigma_\ell(e_i)\sigma_\ell(e_j)\Big]\Big)\\&=\det([\sigma_\ell(e_i)])\det([\sigma_\ell(e_j)])\\&=\det([\sigma_\ell(e_i)])^2.\end{aligned}$$

为证明 $\det([\sigma_\ell(e_i)])\neq0$，我们假定相反. 如果$[\sigma_\ell(e_i)]$是奇异的，存在列矩阵 $C=[c_1,\cdots,c_n]^t\in\hat{E}^n$ 使得 $[\sigma_\ell(e_i)]C=0$. 因此，对 $j=1,\cdots,n$，

$$c_1\sigma_1(e_j)+\cdots+c_n\sigma_n(e_j)=0.$$

由此对 e_i 的每个线性组合 v，

$$c_1\sigma_1(v)+\cdots+c_n\sigma_n(v)=0.$$

但这与特征标的无关性即命题 4.30 矛盾. ■

命题 11.83 设 R 是整闭的，并设 $F=\mathrm{Frac}(R)$. 如果 E/F 是次数为 n 的有限可分域扩张，又如果 $\mathcal{O}=\mathcal{O}_{E/R}$ 是 R 在 E 中的整闭包，则 $\mathcal{O}$ 可以作为子模嵌入一个秩为 n 的自由 R-模.

证明 设 $e_1,\cdots,e_n$ 是 E/F 的基. 根据命题 11.46，对每个 i 存在 $r_i\in R$ 使得 $r_ie_i\in\mathcal{O}$；如有必要改变记号，可假定每个 $e_i\in\mathcal{O}$. 现在系 9.76，它用到双线性型的非退化性，说存在 E 的基 $f_1,\cdots,f_n$ 使得 $t(e_i,f_j)=\mathrm{tr}(e_if_j)=\delta_{ij}$.

设 $\alpha\in\mathcal{O}$. 因 $f_1,\cdots,f_n$ 是基，存在 $c_j\in F$ 使得 $\alpha=\sum c_jf_j$. 对每个 i，其中 $1\leqslant i\leqslant n$，有 $e_i\alpha\in\mathcal{O}$(因为 $e_i\in\mathcal{O}$). 所以根据命题 11.79，$\mathrm{tr}(e_i\alpha)\in R$. 但

$$\begin{aligned}\mathrm{tr}(e_i\alpha)&=\mathrm{tr}\Big(\sum_jc_je_if_j\Big)\\&=\sum_jc_j\,\mathrm{tr}(e_if_j)\\&=c_j\delta_{ij}\\&=c_i.\end{aligned}$$

所以对一切 i，$c_i\in R$，从而 $\alpha=\sum_ic_if_i$ 在以 $f_1,\cdots,f_n$ 为基的自由 R-模中. ■

定义 如果 E 是代数数域，则 $\mathcal{O}_E$ 的一个**整基**是指 $\mathcal{O}_E$ 中的表 $\beta_1,\cdots,\beta_n$ 满足每个 $\alpha\in\mathcal{O}_E$ 有唯一表达式

$$\alpha=c_1\beta_1+\cdots+c_n\beta_n,$$

其中对一切 i，$c_i\in\mathbb{Z}$.

我们现在证明整基恒存在.

命题 11.84 设 E 是代数数域.

⊖ 如果 E/k 是不可分的，则迹形式恒为 0. 见 Isaacs 的《Algebra, A Graduate Course》，369 页.

（i）整数的环 $\mathcal{O}_E$ 有整基，因此它是在加法下有有限秩的自由阿贝尔群．

（ii）$\mathcal{O}_E$ 是诺特整环．

证明 （i）因 $\mathbb{Q}$ 有特征 0，域扩张 $E/\mathbb{Q}$ 是可分的．因此应用命题 11.83 可证明 $\mathcal{O}_E$ 是一个有有限秩的自由 $\mathbb{Z}$-模的子模；即 $\mathcal{O}_E$ 是一个有限生成自由阿贝尔群的子群．根据系 9.4，$\mathcal{O}_E$ 自身是自由阿贝尔群．但 $\mathcal{O}_E$ 的作为自由阿贝尔群的基是一个整基．

（ii）$\mathcal{O}_E$ 中的任一理想 I 是有限生成自由阿贝尔群的子群，因此根据命题 9.7，I 自身是有限生成阿贝尔群．更不必说 I 是有限生成 $\mathcal{O}_E$-模；即 I 是有限生成理想． ■

例 11.85 我们证明 $\mathcal{O}_E$ 未必是 UFD，因此它未必是 PID. 设 $E=\mathbb{Q}(\sqrt{-5})$．因 $-5\equiv 3 \bmod 4$，命题 11.76 给出 $\mathcal{O}_E=\mathbb{Z}[\sqrt{-5}]$．根据例 11.77，$\mathcal{O}_E$ 中的单位只有满足 $N(u)=\pm 1$ 的元素 u．如果 $a^2+5b^2=\pm 1$，其中 $a,b\in\mathbb{Z}$，则 $b=0$ 和 $a=\pm 1$，因此 $\mathcal{O}_E$ 中的单位只有 ± 1．考虑 $\mathcal{O}_E$ 中的因数分解：

$$2\cdot 3=(1+\sqrt{-5})(1-\sqrt{-5}).$$

注意这些因数中的任两个都不相伴（只有 ± 1 是单位），现在证明它们中的每一个都是不可约的．如果 $v\in\mathcal{O}_E$ 整除这四个因数中的任一个（但不是这些因数的相伴数），则 $N(v)$ 是 4，9 或 6 在 $\mathbb{Z}$ 中的真因数，因为 4，9，6 是这些因数的范数（$N(1+\sqrt{-5})=6=N(1-\sqrt{-5})$）．然而立刻可以验证，对于形如 a^2+5b^2 的数在 $\mathbb{Z}$ 中除了 ± 1 再没有这样的因数．所以 $\mathcal{O}_E=\mathbb{Z}[\sqrt{-5}]$ 不是 UFD. ■

迹和范数可以用来求出其他整数的环．

定义 如果 $n\geqslant 2$，则一个**分圆域**是指 $E=\mathbb{Q}(\zeta_n)$，其中 ζ_n 是 n 次单位原根．

回忆一下，如果 p 是素数，则分圆多项式

$$\Phi_p(x)=x^{p-1}+x^{p-2}+\cdots+x+1\in\mathbb{Z}[x]$$

是不可约的，因此 $\operatorname{irr}(\zeta_p,\mathbb{Q})=\Phi_p(x)$ 且 $[\mathbb{Q}(\zeta_p)/\mathbb{Q}]=p-1$．此外，

$$\operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})=\{\sigma_1,\cdots,\sigma_{p-1}\},$$

其中对 $i=1,\cdots,p-1$，$\sigma_i:\zeta_p\mapsto\zeta_p^i$．

我们在 $E=\mathbb{Q}(\zeta_p)$ 中做一些初等计算，使得可以描述 $\mathcal{O}_E$．

引理 11.86 设 p 是奇素数，并设 $E=\mathbb{Q}(\zeta)$，其中 $\zeta=\zeta_p$ 是 p 次单位原根．

（i）$\operatorname{tr}(\zeta^i)=-1, 1\leqslant i\leqslant p-1$．

（ii）$\operatorname{tr}(1-\zeta^i)=p, 1\leqslant i\leqslant p-1$．

（iii）$p=\prod_{i=1}^{p-1}(1-\zeta^i)=N(1-\zeta)$.

（iv）$\mathcal{O}_E(1-\zeta)\cap\mathbb{Z}=p\mathbb{Z}$．

（v）对每个 $u\in\mathcal{O}_E$，$\operatorname{tr}(u(1-\zeta))\in p\mathbb{Z}$．

证明 （i）我们有 $\operatorname{tr}(\zeta)=\sum_{i=1}^{p-1}\zeta^i=\Phi_p(\zeta)-1$，它对每个 p 次单位原根 ζ^i 也成立．由 $\Phi(\zeta)=0$ 可得结果．

（ii）因 $\operatorname{tr}(1)=[E:\mathbb{Q}]=p-1$ 且 tr 是线性函数，

$$\operatorname{tr}(1-\zeta^i)=\operatorname{tr}(1)-\operatorname{tr}(\zeta^i)=(p-1)-(-1)=p.$$

（iii）因 $\Phi(x)=x^{p-1}+x^{p-2}+\cdots+x+1$，有 $\Phi_p(1)=p$．另一方面，p 次单位原根是 $\Phi_p(x)$ 的根，因此

$$\Phi_p(x) = \prod_{i=1}^{p-1}(x - \zeta^i).$$

取$x = 1$处的值得第一个等式．因为各个 $1-\zeta^i$ 都是 $1-\zeta$ 的共轭，所以第二个等式成立．

(iv) 在 (iii) 中的第一个等式表明 $p \in \mathcal{O}_E(1-\zeta) \cap \mathbb{Z}$，因此 $\mathcal{O}_E(1-\zeta) \cap \mathbb{Z} \supseteq p\mathbb{Z}$．如果这个包含关系是严格的，则因 $p\mathbb{Z}$ 是 $\mathbb{Z}$ 中的极大理想，$\mathcal{O}_E(1-\zeta) \cap \mathbb{Z} = \mathbb{Z}$．在这种情形下，$\mathcal{O}_E(1-\zeta) \cap \mathbb{Z} = \mathbb{Z}$，因此 $\mathbb{Z} \subseteq \mathcal{O}_E(1-\zeta)$，从而 $1 \in \mathcal{O}_E(1-\zeta)$．于是有 $v \in \mathcal{O}_E$ 使得 $v(1-\zeta) = 1$；即 $1-\zeta$ 是 $\mathcal{O}_E$ 中的单位．但如果 $1-\zeta$ 是单位，则 $N(1-\zeta) = \pm 1$，与 (iii) 中第二个等式矛盾．

(v) 每个共轭 $\sigma_i(u(1-\zeta)) = \sigma_i(u)(1-\zeta^i)$ 显然在 $\mathcal{O}_E$ 中被 $1-\zeta^i$ 整除．但 $1-\zeta^i$ 在 $\mathcal{O}_E$ 中被 $1-\zeta$ 整除，这是因为

$$1 - \zeta^i = (1-\zeta)(1 + \zeta + \zeta^2 + \cdots + \zeta^{i-1}).$$

因此对一切 i，$\sigma_i(1-\zeta^i) \in \mathcal{O}_E(1-\zeta)$，从而 $\sum_i (u(1-\zeta^i)) \in \mathcal{O}_E(1-\zeta)$．根据系 11.81，$\sum_i (u(1-\zeta)) = \mathrm{tr}(u(1-\zeta))$．根据命题 11.79，$\mathrm{tr}(u(1-\zeta)) \in \mathbb{Z}$，所以根据 (iv)，$\mathrm{tr}(u(1-\zeta)) \in \mathcal{O}_E(1-\zeta) \cap \mathbb{Z} = p\mathbb{Z}$． ■

命题 11.87 *如果 p 是奇素数和 $E = \mathbb{Q}(\zeta_p)$ 是分圆域，则*

$$\mathcal{O}_E = \mathbb{Z}[\zeta_p].$$

证明 我们把 ζ_p 缩写为 ζ．$\mathbb{Z}[\zeta] \subseteq \mathcal{O}_E$ 总是成立的，我们现在证明反包含成立．根据引理 11.74，每个元素 $u \in \mathcal{O}_E$ 有表达式

$$u = c_0 + c_1\zeta + c_2\zeta^2 + \cdots + c_{p-2}\zeta^{p-2},$$

其中 $c_i \in \mathbb{Q}$（记住 $[E:\mathbb{Q}] = p-1$）．我们必须证明对一切 i，$c_i \in \mathbb{Z}$．乘以 $1-\zeta$ 得

$$u(1-\zeta) = c_0(1-\zeta) + c_1(\zeta - \zeta^2) + \cdots + c_{p-2}(\zeta^{p-2} - \zeta^{p-1}).$$

根据 (i)，对于 $1 \leqslant i \leqslant p-2$，$\mathrm{tr}(\zeta^i - \zeta^{i+1}) = \mathrm{tr}(\zeta^i) - \mathrm{tr}(\zeta^{i+1})$，从而 $\mathrm{tr}(u(1-\zeta)) = c_0\mathrm{tr}(1-\zeta)$；因为根据 (ii)，$\mathrm{tr}(1-\zeta) = p$，所以 $\mathrm{tr}(u(1-\zeta)) = pc_0$．另一方面，根据 (iv)，$\mathrm{tr}(u(1-\zeta)) \in p\mathbb{Z}$．因此有某个 $m \in \mathbb{Z}$ 使得 $pc_0 = mp$，从而 $c_0 \in \mathbb{Z}$．现在 $\zeta^{-1} = \zeta^{p-1} \in \mathcal{O}_E$，因此

$$(u - c_0)\zeta^{-1} = c_1 + c_2\zeta + \cdots + c_{p-2}\zeta^{p-3} \in \mathcal{O}_E.$$

刚才给出的论证表明 $c_1 \in \mathbb{Z}$．事实上，重复这个论证可以证明一切 $c_i \in \mathbb{Z}$，因此 $u \in \mathbb{Z}[\zeta]$． ■

在离开这个有趣的课题之前，我们必须提起狄利克雷的一个优美定理．下面陈述的证明见 Samuel 所著的《Algebraic Theory of Numbers》第 4 章．一个次数为 n 的代数数域 E 恰有 n 个到 $\mathbb{C}$ 中的嵌入．如果 r_1 是象在 $\mathbb{R}$ 中的这种嵌入的个数，则 $n - r_1$ 是偶数；比如 $n - r_1 = 2r_2$．

定理（狄利克雷单位定理） *设 E 是次数为 n 的代数数域．则 $n = r_1 + 2r_2$（其中 r_1 是 E 到 $\mathbb{R}$ 中的嵌入的个数），且 $\mathcal{O}_E$ 中单位的乘法群 $U(\mathcal{O}_E)$ 是有限生成阿贝尔群．精确地说，*

$$U(\mathcal{O}_E) \cong \mathbb{Z}^{r_1+r_2-1} \times T,$$

其中 T 是由 E 中的单位根组成的有限循环群．

习题

11.41 (i) 如果 $E = \mathbb{Q}(\sqrt{-3})$，证明 $\mathcal{O}_E$ 中的单位只有

$$\pm 1, \frac{1}{2}(1 \pm \sqrt{-3}), \frac{1}{2}(-1 \pm \sqrt{-3}),$$

(ii) 设 d 是负的无平方因数的整数且 $d \neq -1$ 和 $d \neq -3$．如果 $E = \mathbb{Q}(\sqrt{d})$，证明 $\mathcal{O}_E$ 中的单位只有

± 1.

11.42 (i) 证明：如果 $E = \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$，则没有单位 $u \in \mathcal{O}_E$ 满足 $1 < u < 1+\sqrt{2}$.

(ii) 如果 $E = \mathbb{Q}(\sqrt{2})$，证明 $\mathcal{O}_E$ 有无限个单位.

提示：用 (i) 证明 $1+\sqrt{2}$ 的一切幂都是不同的.

定义：如果 $\alpha_1, \cdots, \alpha_n$ 是代数数域 E 中的整数环 $\mathcal{O}_E$ 的一个整基，则判别式是

$$\Delta(\mathcal{O}_E) = \det[\operatorname{tr}(\alpha_i \alpha_j)]$$

(可以证明这个定义不依赖于整基的选取).

11.43 设 d 是无平方因数的整数，并设 $E = \mathbb{Q}(\sqrt{d})$.

(i) 如果 $d \equiv 2 \bmod 4$ 或 $d \equiv 3 \bmod 4$，证明 $1, \sqrt{d}$ 是 $\mathcal{O}_E$ 的整基，并证明 $\mathcal{O}_E$ 的一个判别式是 $4d$.

(ii) 如果 $d \equiv 1 \bmod 4$，证明 $1, \frac{1}{2}(1+\sqrt{d})$ 是 $\mathcal{O}_E$ 的整基，并证明 $\mathcal{O}_E$ 的一个判别式是 d.

11.44 设 p 是奇素数，并设 $E = \mathbb{Q}(\zeta_p)$ 是分圆域.

(i) 证明 $1, 1-\zeta_p, (1-\zeta_p)^2, \cdots, (1-\zeta_p)^{p-2}$ 是 $\mathcal{O}_E$ 的整基.

(ii) 证明 $\mathcal{O}_E$ 的一个判别式是 $(-1)^{\frac{1}{2}(p-1)} p^{p-2}$.

提示：见 Pollard 所著的《The Theory of Algebraic Numbers》第 67 页.

11.45 (i) 如果 $\mathbb{A}$ 是一切代数数的域，证明 $\mathcal{O}_{\mathbb{A}}$ 不是诺特环.

(ii) 证明 $\mathcal{O}_{\mathbb{A}}$ 中的每个非零素理想都是极大理想.

提示：用系 11.53 的证明.

11.2.4 戴得金环的刻画

下面的定义涉及代数数域 E 中的整数环 $\mathcal{O}_E$ 所具有的一些环论性质.

定义 *如果整环 R 是整闭的、诺特的，且它的非零素理想是极大理想，则称 R 为*戴得金环.

例 11.88 (i) 根据命题 11.46、命题 11.84 和系 11.53，代数数域 E 中的环 $\mathcal{O}_E$ 是戴得金环.

(ii) 每个主理想整环 R 是戴得金环. ■

在例 11.85 中已经证明 $R = \mathbb{Z}[\sqrt{-5}]$ 是戴得金环，但它不是 UFD，因此它不是 PID. 我们提醒读者，库默尔在 19 世纪 40 年代研究费马最后定理时认识到这种例子，他附加“理想”数到整数环中以迫使因子分解唯一. 大约 30 年之后，戴得金引入现代的理想定义，并证明库默尔的理想数相当于戴得金的理想. 在定理 11.95 中，我们将证明在戴得金环中，每个非零理想可以唯一地分解为素理想的积.

我们现在刻画 DVR，然后证明戴得金环的局部化有良好的性态.

引理 11.89 *整环 R 是 DVR 当且仅当它是诺特的、整闭的且有唯一非零素理想.*

证明 如果 R 是 DVR，则它有所要求的性质（回忆 R 是 PID，因此它是整闭的）.

逆命题要求证明 R 是 PID，这不是像期望的那样简单. 设 $\mathfrak{p}$ 是非零素理想，选取非零元素 $a \in \mathfrak{p}$. 定义 $M = R/Ra$，考虑一切零化子 $\operatorname{ann}(m)$ 的族 $\mathcal{A}$，m 遍历 M 的一切非零元素. 因 R 是诺特环，它满足极大条件，因此存在非零元素 $b + Ra \in M$，它的零化子 $\mathfrak{q} = \operatorname{ann}(b+Ra)$ 在 $\mathcal{A}$ 中极大. 我们断言 $\mathfrak{q}$ 是素理想. 假设 $x, y \in R$，$xy \in \mathfrak{q}$，$x, y \notin \mathfrak{q}$. 则因 $y \notin \mathfrak{q}$，$y(b+Ra) = yb + Ra$ 是 M 的非零元素. 但因 $x \notin \operatorname{ann}(b+Ra)$，$\operatorname{ann}(yb+Ra) \supsetneq \operatorname{ann}(b+Ra)$，与 $\mathfrak{q}$ 的极大性矛盾. 所以 $\mathfrak{q}$ 是素理想. 因 R 有唯一非零素理想 $\mathfrak{p}$，有

$$\mathfrak{q} = \text{ann}(b + Ra) = \mathfrak{p}.$$

注意

$$b/a \notin R.$$

否则，$b + Ra = 0 + Ra$，与 $b + Ra$ 是 $M = R/Ra$ 的非零元素矛盾．

现在证明 $\mathfrak{p}$ 是主理想，生成元为 a/b（我们不知道 $a/b \in \text{Frac}(R)$ 是否在 R 中）．首先，有 $\mathfrak{p}b = \mathfrak{q}b \subseteq Ra$，因此 $\mathfrak{p}(b/a) \subseteq R$；即 $\mathfrak{p}(b/a)$ 是 R 中的理想．如果 $\mathfrak{p}(b/a) \subseteq \mathfrak{p}$，则 b/a 是 R 上的整元，这是因为 $\mathfrak{p}$ 是 $\text{Frac}(R)$ 的有限生成 R-子模，正如引理 11.41 所要求的．由于 R 是整闭的，从而 $b/a \in R$，与上段末尾的注记矛盾．所以 $\mathfrak{p}(b/a)$ 不是真理想，从而 $\mathfrak{p}(b/a) = R$ 和 $\mathfrak{p} = R(a/b)$．由此 $a/b \in R$，$\mathfrak{p}$ 是主理想．

记 a/b 为 t．我们证明 R 中的非零理想只有 t^n 生成的主理想，其中 $n \geqslant 0$，由此本引理的证明就得以完成．设 I 是 R 中的非零理想，考虑 $\text{Frac}(R)$ 的子模的链：

$$I \subseteq It^{-1} \subseteq It^{-2} \subseteq \cdots.$$

我们断言这个链是严格递增的．如果 $It^{-n} = It^{-n-1}$，则有限生成 R-模 It^{-1} 满足 $t^{-1}(It^{-n}) \subseteq It^{-n}$，因此 $t^{-1} = b/a$ 是 R 上的整元．和上面一样，R 整闭迫使 $b/a \in R$，这是一个矛盾．因 R 是诺特环，这个链只能含有 R 中有限个理想．于是存在 n 使得 $It^{-n} \subseteq R$ 而 $It^{-n-1} \not\subseteq R$．如果 $It^{-n} \subseteq \mathfrak{p} = Rt$，则 $It^{-n-1} \subseteq R$，产生矛盾．所以 $It^{-n} = R$ 且正如所要的有$I = Rt^n$． ■

命题 11.90 *如果 R 是诺特整环，则 R 是戴得金环当且仅当对每个非零素理想 $\mathfrak{p}$，局部化 $R_\mathfrak{p}$ 是 DVR.*

注 *习题 11.45 表明必须假定 R 是诺特环．*

证明 如果 R 是戴得金环和 $\mathfrak{p}$ 是极大理想，系11.18(ⅳ)证明 $R_\mathfrak{p}$ 有唯一非零素理想．此外，$R_\mathfrak{p}$ 是诺特环（系11.18(ⅴ)）、整环（系11.16）和整闭的（习题 11.26）．根据引理 11.89，$R_\mathfrak{p}$ 是 DVR.

关于逆命题，我们必须证明 R 是整闭的且它的非零素理想是极大的．设 $u/v \in \text{Frac}(R)$ 是 R 上的整元．对每个非零素理想 $\mathfrak{p}$，元素 u/v 是 $R_\mathfrak{p}$ 上的整元（注意 $\text{Frac}(R_\mathfrak{p}) = \text{Frac}(R)$）．但 $R_\mathfrak{p}$ 是 PID，因此是整闭的，从而 $u/v \in R_\mathfrak{p}$．由此根据命题 11.20，$u/v \in \bigcap_\mathfrak{p} R_\mathfrak{p} = R$．所以 R 是整闭的．

假设在 R 中存在非零素理想 $\mathfrak{p} \subsetneq \mathfrak{q}$．根据系11.18(ⅳ)，在 $R_\mathfrak{q}$ 中 $\mathfrak{p}_\mathfrak{q} \subsetneq \mathfrak{q}_\mathfrak{q}$．这与 DVR 有唯一非零素理想的事实矛盾．所以非零素理想是极大的，因此 R 是戴得金环． ■

设 R 是整环且 $F = \text{Frac}(R)$，并设 $I = Ra$ 是 R 中的非零主理想．如果定义 $J = Ra^{-1} \subseteq F$，它是由 a^{-1} 生成的循环 R-子模，则易知

$$IJ = \{uv : u \in I, v \in J\} = R.$$

定义 *如果 R 是整环且 $F = \text{Frac}(R)$，则***分式理想***是指 F 的一个有限生成非零 R-子模．如果 I 是非零分式理想，则*

$$I^{-1} = \{v \in F : vI \subseteq R\}.$$

$I^{-1}I \subseteq R$ 是恒成立的；称分式理想 I **可逆**，*如果 $I^{-1}I = R$.*

R 中的每个有限生成理想也是一个分式理想．在这个背景下，当我们要把这种理想（它是通常的理想!）和更一般的分式理想比较的时候，常称这种理想为**整理想**．

我们断言，如果$I = Ra$ 是 R 中的非零主理想，则$I^{-1} = Ra^{-1}$．显然，对一切 $r' \in R$，$(ra^{-1})(r'a) = rr' \in R$，因此 $Ra^{-1} \subseteq I^{-1}$．关于反包含，假设 $(u/v)a \in R$，其中 $u, v \in R$．则在 R 中 $v \mid ua$，从

而存在 $r \in R$ 使得 $rv = ua$. 因此在 F 中有 $u = rva^{-1}$，从而 $u/v = (rva^{-1})/v = ra^{-1}$. 所以 R 中的每个非零主理想是可逆的.

引理 11.91 如果 R 是整环且 $F = \mathrm{Frac}(R)$，则分式理想 I 是可逆的当且仅当存在 $a_1, \cdots, a_n \in I$ 和 $q_1, \cdots, q_n \in F$ 使得

（ⅰ）对 $i = 1, \cdots, n, q_i I \subseteq R$；

（ⅱ）$1 = \sum_{i=1}^{n} q_i a_i$.

证明 如果 I 是可逆的，则 $I^{-1}I = R$. 因 $1 \in I^{-1}I$，存在 $a_1, \cdots, a_n \in R$ 和 $q_1, \cdots, q_n \in I^{-1}$ 使得 $1 = \sum_i q_i a_i$. 因 $q_i \in I^{-1}$，有 $q_i I \subseteq R$.

为证明逆命题，假定由 $q_1, \cdots, q_n$ 生成的 R-子模 J 是分式理想. 因 $1 = \sum_{i=1}^{n} q_i a_i \in JI$，$JI$ 是包含 1 的 R 的 R-子模；即 $JI = R$. 要证明 I 是可逆的，剩下的只需证明 $J = I^{-1}$. 显然每个 $q_i \in I^{-1}$，从而 $J \subseteq I^{-1}$. 关于反包含，假定 $u \in F$ 和 $uI \subseteq R$. 因 $1 = \sum_i q_i a_i$，对一切 i 有 $ua_i \in R$，所以 $u = \sum_i (ua_i) q_i \in J$. ■

系 11.92 整环 R 中的每个可逆理想 I 都是有限生成的.

证明 因 I 是可逆的，存在引理中那样的 $a_1, \cdots, a_n \in I$ 和 $q_1, \cdots, q_n \in F$. 如果 $b \in I$，则因 $bq_i \in R$，所以有 $b = b1 = \sum_i bq_i a_i \in I$. 所以 I 由 $a_1, \cdots, a_n \in I$ 生成. ■

命题 11.93 对于整环 R 下面的条件等价.

（ⅰ）R 是戴得金环.

（ⅱ）每个分式理想都是可逆的.

（ⅲ）一切分式理想的集合 $\mathcal{F}(R)$ 在理想的乘法下形成阿贝尔群.

证明 （ⅰ）⇒（ⅱ）. 设 J 是 R 中的分式理想. 因 R 是戴得金环，它的局部化 $R_\mathfrak{p}$ 是 PID，从而 $J_\mathfrak{p}$ 和每个非零主理想一样是可逆的（在定理 9.3 中，为证明有限生成无挠阿贝尔群是自由阿贝尔群，我们实际上证明了 PID 的分式理想是循环模）. 现在习题 11.50 给出

$$(J^{-1}J)_\mathfrak{p} = (J^{-1})_\mathfrak{p} J_\mathfrak{p} = (J_\mathfrak{p})^{-1} J_\mathfrak{p} = R_\mathfrak{p}.$$

命题 11.30 给出 $J^{-1}J = R$，因此 J 是可逆的.

（ⅱ）⇔（ⅲ）. 如果 $I, J \in \mathcal{F}(R)$，则根据系 11.92，它们是有限生成的，且

$$IJ = \{ \sum a_\ell b_\ell : a_\ell \in I \text{ 和 } b_\ell \in J \}$$

是 $\mathrm{Frac}(R)$ 的有限生成 R-子模. 如果 $I = (a_1, \cdots, a_n)$ 和 $J = (b_1, \cdots, b_m)$，则 IJ 由一切 $a_i b_j$ 生成. 因此 IJ 是有限生成的且 $IJ \in \mathcal{F}(R)$. 结合性成立，幺元是 R，分式理想 J 的逆是 J^{-1}，这是因为 J 是可逆的. 由此 $\mathcal{F}(R)$ 是阿贝尔群.

反之，如果 $\mathcal{F}(R)$ 是阿贝尔群且 $I \in \mathcal{F}(R)$，则存在 $J \in \mathcal{F}(R)$ 使得 $JI = R$. 我们需要证明 $J = I^{-1}$. 但

$$R = JI \subseteq I^{-1}I \subseteq R,$$

因此 $JI = I^{-1}I$. 在群 $\mathcal{F}(R)$ 中消去 I 得所要得 $J = I^{-1}$.

（ⅲ）⇒（ⅰ）. 首先，因为（ⅲ）⇒（ⅱ）表明每个非零理想 I 是可逆的，而且系 11.92 证明

I 是有限生成的，所以 R 是诺特环．

其次，我们证明每个非零素理想 $\mathfrak{p}$ 是极大理想．设 I 是理想满足 $\mathfrak{p} \subsetneq I$（允许 $I = R$）．则 $\mathfrak{p}I^{-1} \subseteq II^{-1} = R$，因此 $\mathfrak{p}I^{-1}$ 是 R 中的（整）理想．现在因为 $\mathcal{F}(R)$ 中的乘法是结合的，所以 $(\mathfrak{p}I^{-1})I = \mathfrak{p}$．因 $\mathfrak{p}$ 是素理想，命题 6.13 说 $\mathfrak{p}I^{-1} \subseteq \mathfrak{p}$ 或 $I \subseteq \mathfrak{p}$．第二种情形不可能成立，因此 $\mathfrak{p}I^{-1} \subseteq \mathfrak{p}$．乘以 $\mathfrak{p}^{-1}I$ 得 $R \subseteq I$．所以 $I = R$，因此 $\mathfrak{p}$ 是极大理想．

第三，如果 $a \in \mathrm{Frac}(R)$ 是 R 上的整元，则引理 11.41 给出 $\mathrm{Frac}(R)$ 的有限生成 R-子模 J，也就是一个分式理想，使得 $aJ \subseteq J$．因 J 是可逆的，存在 $q_1, \cdots, q_n \in \mathrm{Frac}(R)$ 和 $a_1, \cdots, a_n \in J$ 使得对一切 i 有 $q_iJ \subseteq R$ 且 $1 = \Sigma q_ia_i$．因此 $a = \sum_i q_ia_ia$．但 $a_ia \in J$ 和 $q_iJ \subseteq R$ 给出 $a = \sum_i q_i(a_ia) \in R$. 所以 R 是整闭的，因此它是戴得金环． ■

命题 11.94 （ⅰ）*如果 R 是 UFD，则 R 中的非零理想 I 是可逆的当且仅当它是主理想．*

（ⅱ）*戴得金环是 UFD 当且仅当它是 PID.*

证明 （ⅰ）我们已经知道每个非零主理想是可逆的．反之，如果 I 是可逆的，存在元素 $a_1, \cdots, a_n \in I$ 和 $q_1, \cdots, q_n \in \mathrm{Frac}(R)$ 使得 $1 = \sum_i q_ia_i$ 且对一切 i，$q_iI \subseteq R$．设 $q_i = b_i/c_i$，其中 b_i，$c_i \in R$．因 R 是 UFD，可以假定 q_i 是既约的；即 $(b_i, c_i) = 1$．但 $(b_i/c_i)a_j \in R$ 说 $c_i \mid b_ia_j$，因此根据习题6.18(ⅰ)，对一切 i，j，$c_i \mid a_j$．我们断言 $I = Rc$，其中 $c = \mathrm{lcm}\{c_1, \cdots, c_n\}$．首先，因为 $cb_i/c_i \in R$ 和 $c = c1 = \sum_i (cb_i/c_i)a_i$ 有 $c \in I$．因此 $Rc \subseteq I$．关于反包含，习题6.18(ⅱ)证明对一切 j，$c \mid a_j$，从而对一切 j 有 $a_j \in Rc$，因此 $I \subseteq Rc$．

（ⅱ）因戴得金环中的每个非零理想都是可逆的，由(ⅰ)，如果 R 是 UFD，则 R 中的每个理想都是主理想． ■

定义 *如果 R 是戴得金环，则它的***类群** *$C(R)$ 由*

$$C(R) = \mathcal{F}(R)/\mathcal{P}(R)$$

定义，其中 $\mathcal{P}(R)$ 是一切非零主理想的子群．

狄利克雷证明，对每个代数数域 E，$C(\mathcal{O}_E)$ 的类群是有限的；阶 $|C(R)|$ 叫做 $\mathcal{O}_E$ 的**类数**．通常用闵可夫斯基的一个几何定理证明类数的有限性，这个定理说欧几里得空间中的充分大的平行六面体必包含格点（见 Samuel 所著的《Algebraic Theory of Numbers》，57～58 页）．

L. Claborn 证明，对每个（未必有限的）阿贝尔群 G，存在戴得金环 R 使得 $C(R) \cong G$．

我们现在证明库默尔和戴得金的结果之间有关联的结论．

定理 11.95 *如果 R 是戴得金环，则每个真非零理想有分解为素理想之积的唯一因子分解．逆命题也成立．*

证明 设$\mathcal{S}$是 R 中不是素理想之积的一切真非零理想的族．如果 $\mathcal{S} = \varnothing$，则 R 中的每个非零理想都是素理想的积．如果 $\mathcal{S} \neq \varnothing$，则因诺特环满足极大条件（命题 6.38），$\mathcal{S}$有极大元素 I．现在 I 不可能是 R 中的极大理想，因为一个"素理想之积"允许这个积只有一个因子．设 $\mathfrak{m}$ 是包含 I 的极大理想．因 $I \subsetneq \mathfrak{m}$，有 $\mathfrak{m}^{-1}I \subsetneq \mathfrak{m}^{-1}\mathfrak{m} = R$；即 $\mathfrak{m}^{-1}I$ 是真包含 I 的真理想．因为 $\mathfrak{m}$ 和 $\mathfrak{m}^{-1}I$ 都严格地大于$\mathcal{S}$中的极大元素 I，所以 $\mathfrak{m}$ 和 $\mathfrak{m}^{-1}I$ 都不在$\mathcal{S}$中，从而它们中的每一个都是素理想之积. 因此 $I = \mathfrak{m}(\mathfrak{m}^{-1}I)$（等式成立是因为 R 是戴得金环）是素理想之积，与 I 在$\mathcal{S}$中矛盾．所以 $\mathcal{S} = \varnothing$，且 R 中的每个真非零理想都是素理想之积．

假设 $\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$，其中 $\mathfrak{p}_i$ 和 $\mathfrak{q}_j$ 都是素理想．我们对 $\max\{r, s\}$ 用归纳法证明因子分解的唯

一性．基础步 $r=1=s$ 显然为真．关于归纳步，注意 $\mathfrak{p}_1 \supseteq \mathfrak{q}_1 \cdots \mathfrak{q}_s$，因此命题 6.13 给出 $\mathfrak{q}_j$ 使得 $\mathfrak{p}_1 \supseteq \mathfrak{q}_j$．因为素理想是极大理想，所以 $\mathfrak{p}_i = \mathfrak{q}_j$．现在原始等式乘以 $\mathfrak{p}_1^{-1}$ 再用归纳假设即可． ■

系 11.96 如果 R 是戴得金环，则 $\mathcal{F}(R)$ 是以一切非零素理想为基的自由阿贝尔群．

证明 当然 $\mathcal{F}(R)$ 是写成乘性的．每个分式理想都是素理想的积表明素理想的集合生成 $\mathcal{F}(R)$；因子分解的唯一性说明素理想的集合是基． ■

根据定理 11.95，算术的许多常用公式可以推广到戴得金环中的理想上．在 $\mathbb{Z}$ 中，理想(3)包含理想 (9)．事实上，$\mathbb{Z}m \supseteq \mathbb{Z}n$ 当且仅当 $m \mid n$．我们现在将看到对于理想的“包含”关系相当于“整除”，且 gcd 和 lcm 的通常公式（命题 1.17）可以推广到戴得金环上．

命题 11.97 设 I 和 J 都是戴得金环 R 中的非零理想，并设它们的素因子分解是

$$I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n} \quad 和 \quad J = \mathfrak{p}_1^{f_1} \cdots \mathfrak{p}_n^{f_n},$$

其中对一切 i，$e_i \geqslant 0$ 和 $f_i \geqslant 0$．

（i）$J \supseteq I$ 当且仅当有某个理想 L 使得 $I = JL$．

（ii）$J \supseteq I$ 当且仅当对一切 i，$f_i \leqslant e_i$．

（iii）如果 $m_i = \min\{e_i, f_i\}$ 和 $M_i = \max\{e_i, f_i\}$，则

$$I \cap J = \mathfrak{p}_1^{M_1} \cdots \mathfrak{p}_n^{M_n} \quad 和 \quad I + J = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_n^{m_n}.$$

特别地，$I + J = R$ 当且仅当对一切 i，$\min\{e_i, f_i\} = 0$．

（iv）设 R 是戴得金环，并设 $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$ 是 R 中的非零理想．则

$$R/I = R/\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n} \cong (R/\mathfrak{p}_1^{e_1}) \times \cdots \times (R/\mathfrak{p}_n^{e_n}).$$

证明 （i）如果 $I \subseteq J$，则 $J^{-1}I \subseteq R$，且

$$J(J^{-1}I) = I.$$

反之，如果 $I = JL$，则因 $JL \subseteq JR = J$，所以 $I \subseteq J$．

（ii）由（i）和非零理想作为素理想之积的唯一因子分解可得结果．

（iii）我们对 $I+J$ 证明公式．设 $I+J = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n}$ 并设 $A = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_n^{m_n}$．因 $I \subseteq I+J$ 和 $J \subseteq I+J$，有 $r_i \leqslant e_i$ 和 $r_i \leqslant f_i$，从而 $r_i \leqslant \min\{e_i, f_i\} = m_i$．因此 $A \subseteq I+J$．关于反包含，$A \subseteq I$ 和 $A \subseteq J$，因此根据（i），有理想 I' 和 J' 使得 $A = II'$ 和 $A = JJ'$．所以 $I+J = AI' + AJ' = A(I'+J')$，从而 $I+J \subseteq A$．对 IJ 的公式的证明留给读者．

（iv）这正是孙子剩余定理，即习题6.11(iii)，因此只需验证当 $i \neq j$ 时，$\mathfrak{p}_i^{e_i}$ 和 $\mathfrak{p}_j^{e_j}$ 互素；即 $\mathfrak{p}_i^{e_i} + \mathfrak{p}_j^{e_j} = R$. 但这由（iii）得到． ■

回忆命题 7.58：R-模 A 是投射的当且仅当它有投射基：存在元素 $\{a_j : J \in J\} \subseteq A$ 和 R-映射 $\{\varphi_j : A \to R : j \in J\}$ 满足

（i）对每个 $x \in A$，几乎一切 $\varphi_j(x) = 0$；

（ii）对每个 $x \in A$，$x = \sum_{j \in J} (\varphi_j x) a_j$．

命题 11.98 （i）整环 R 中的非零理想 I 是可逆的当且仅当 I 是投射 R-模．

（ii）整环 R 是戴得金环当且仅当 R 中的每个理想都是投射的．

证明 (i) 如果 I 是可逆的，存在元素 $a_1, \cdots, a_n \in I$ 和 $q_1, \cdots, q_n \in \mathrm{Frac}(R)$ 使得 $1 = \sum_i q_i a_i$ 且对一切 i，$q_i I \subset R$．定义 $\varphi_i : I \to R$ 为 $\varphi_i : a \mapsto q_i a$（注意，因为 $q_i I \subseteq R$，所以 $\mathrm{im}\varphi_i \subseteq I$）．如果 $a \in I$，则

$$\sum_i \varphi_i(a)a_i = \sum_i q_i a a_i = a\sum_i q_i a_i = a.$$

所以 I 有投射基，因此 I 是投射 R-模．

反之，如果 I 是投射的，它有投射基 $\{\varphi_j : j \in J\}$，$\{a_j : j \in J\}$．如果 $b \in I$ 非零，定义 $q_j \in \mathrm{Frac}(R)$ 为

$$q_j = \varphi_j(b)/b.$$

这个元素不依赖于非零 b 的选取：如果 $b' \in I$ 非零，则 $b'\varphi_j(b) = \varphi_j(b'b) = b\varphi_j(b')$，因此 $\varphi_j(b)/b = \varphi_j(b')/b'$．为证明 $q_j I \subseteq R$，注意，如果 $b \in I$ 非零，则 $q_j b = (\varphi_j(b)/b)b = \varphi_j(b) \in R$．根据投射基定义中的（ⅰ），几乎一切 $\varphi_j(b) = 0$，因此只有有限个非零 $q_j = \varphi_j(b)/b$（记住 q_j 不依赖于非零 $b \in I$ 的选取）．投射基定义中的（ⅱ）给出，对 $b \in I$，

$$b = \sum_j \varphi_j(b)a_j = \sum_j (q_j b)a_j = b\Big(\sum_j q_j a_j\Big).$$

消去 b 得 $1 = \sum_j q_j a_j$．最后，具有满足 $q_j \neq 0$ 的那些指标 j 的 a_j 的集合备齐了证明 I 是可逆理想的必需资料．

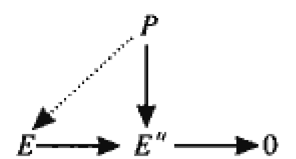
（ⅱ）由（ⅰ）和命题 11.93 立得．■

例 11.99　我们已经知道 $R = \mathbb{Z}[\sqrt{-5}]$ 为不是 PID 的戴得金环．任一非主理想给出不是自由的投射 R-模的例子．■

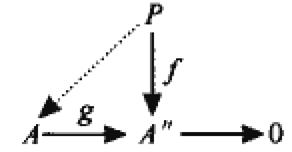
注　如果一个未必交换的环 R 的每个左理想都是投射 R-模，则称 R 为**左遗传**的（存在不是右遗传的左遗传环）．左遗传环的一些例子中除了戴得金环之外还有半单环、非交换主理想环和 FIR（自由理想环——一切左理想都是自由 R-模）. P. M. Cohn 证明域上变量不交换的多项式环是 FIR，因此存在不是左诺特环的左遗传环．

戴得金环上的投射和内射模具有良好的性态．

引理 11.100　*左 R-模 P（在任意环 R 上）是投射的当且仅当每个下面有内射模 E 的图能够补全成为一个交换图．内射模的对偶刻画也成立．*



证明　如果 P 是投射的，则对每个未必是内射的模 E，图都能补全．反之，我们需要证明图



对任意模 A 和任意满射 $g : A \to A''$ 都能补全．根据定理 8.104，存在内射 R-模 E 和内射 $\sigma : A \to E$．定义 $E'' = \mathrm{coker}\,\sigma i = E/\mathrm{im}\,\sigma i$，并考虑行正合的交换图

$$\begin{array}{ccccccccc} 0 & \to & A' & \xrightarrow{i} & A & \xrightarrow{g} & A'' & \to & 0 \\ & & \downarrow{1_{A'}} & & \downarrow{\sigma} & & \downarrow{h} & & \\ 0 & \to & A' & \xrightarrow{\sigma i} & E & \xrightarrow{\nu} & E'' & \to & 0 \end{array}$$

（图中 P 位于上方，$f : P \to A''$，$\pi : P \to E$。）

其中 $\nu: E \to E'' = \mathrm{coker}\,\sigma i$ 是自然映射，且根据命题 8.93，$h: A'' \to E''$ 存在．根据假设，存在映射 $\pi: P \to E$ 使得 $\nu\pi = hf$．我们断言 $\mathrm{im}\pi \subseteq \mathrm{im}\sigma$．对 $x \in P$，g 的满射性给出 $a \in A$ 使得 $ga = fx$．于是 $\nu\pi x = hfx = hga = \nu\sigma a$，从而 $\pi x - \sigma a \in \ker\nu = \mathrm{im}\sigma i$；因此有某个 $a' \in A$ 使得 $\pi x - \sigma a = \sigma i a'$，从而 $\pi x = \sigma(a + ia') \in \mathrm{im}\sigma$. 所以，如果 $x \in P$，则存在唯一的 $a \in A$ 使得 $\sigma a = \pi x$（因为 σ 是内射，所以 a 是唯一的）．于是，存在合理定义的函数 $\pi': P \to A$，它由 $\pi' x = a$ 给出，其中 $\sigma a = \pi x$. 读者可以验证 π' 是 R-映射和 $g\pi' = j$． ■

定理 11.101（嘉当-艾伦伯格） 对整环 R，下面的条件等价：

（i）R 是戴得金环．

（ii）投射 R-模的每个子模都是投射的．

（iii）内射 R-模的每个商都是内射的．

证明 （i）⇔（ii）. 如果 R 是戴得金环，则可以修改定理 9.8（该定理证明自由阿贝尔群的每个子群也是自由阿贝尔群）的证明来证明自由 R-模的每个子模是投射的（见习题 11.47）；特别地，投射 R-模的每个子模是投射的．反之，因 R 自身是投射 R-模，根据假设，它的子模也是投射的；即 R 的理想是投射的．现在命题 11.98 证明 R 是戴得金环．

（ii）⇔（iii）. 假定（iii）成立，考虑行正合的图

$$\begin{array}{ccccc} P & \leftarrow & P' & \leftarrow & 0 \\ \downarrow & \searrow & \downarrow f & & \\ E & \rightarrow & E'' & \rightarrow & 0 \end{array}$$

其中 P 是投射的而 E 是内射的；注意假设给出 E'' 是内射的．为证明 P' 的投射性，根据引理 11.100，只需求出映射 $P' \to E$ 使得图交换．因 E'' 是内射的，存在满足交换性的映射 $P \to E''$．因 P 是投射的，也存在满足交换性的映射 $P \to E$．复合 $P' \to P \to E$ 是所要的映射．逆命题是这个论证的对偶，用引理 11.100 的对偶命题即可． ■

系 11.102 设 R 是戴得金环．

（i）对一切 R-模 C 和 A，对一切 $n \geqslant 2$ 有

$$\mathrm{Ext}^n_R(C,A) = \{0\} \quad 和 \quad \mathrm{Tor}^R_n(C,A) = \{0\}.$$

（ii）设 $0 \to A' \to A \to A'' \to 0$ 是短正合列．对每个模 C，存在正合列

$$0 \to \mathrm{Hom}(C,A') \to \mathrm{Hom}(C,A) \to \mathrm{Hom}(C,A'')$$
$$\to \mathrm{Ext}^1(C,A') \to \mathrm{Ext}^1(C,A) \to \mathrm{Ext}^1(C,A'') \to 0$$

和

$$0 \to \mathrm{Tor}^R_1(C,A') \to \mathrm{Tor}^R_1(C,A) \to \mathrm{Tor}^R_1(C,A'')$$
$$\to C \otimes_R A' \to C \otimes_R A \to C \otimes_R A'' \to 0.$$

证明 （i）根据定义，如果

$$\cdots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \to C \to 0$$

是 C 的投射分解，则

$$\mathrm{Ext}^n(C,A) = \ker d^*_{n+1} / \mathrm{im}\, d^*_n\ ;$$

此外，根据系 10.74，$\mathrm{Ext}^n(C,A)$ 不依赖于投射分解的选取．现在 C 是自由模 F 的商，因此存在正合列

$$0 \to K \to F \xrightarrow{\varepsilon} C \to 0, \tag{5}$$

其中 $K=\ker\varepsilon$．因 R 是戴得金环，自由 R-模 F 的子模 K 是投射的，因此(5)定义了 C 的一个投射分解，其中 $P_0=F, P_1=K$ 且对一切 $n\geqslant 2$，$P_n=\{0\}$．因此，对一切 $n\geqslant 2$，$\ker d_{n+1}^*\subseteq \mathrm{Hom}(P_n,A)=\{0\}$，从而对一切 A 和一切 $n\geqslant 2$，$\mathrm{Ext}_R^n(C,A)=\{0\}$. 对 Tor 可作类似的论证．

（ⅱ）分别由系 10.68 和系 10.57，即 Ext 和 Tor 的长正合列可得结果． ■

下节中要用这些结果推广命题 10.92.

习题

11.46 设 R 是交换环并设 M 是有限生成 R-模．证明：如果对 R 中的某个理想 I，$IM=M$，则存在 $a\in I$ 使得 $(1-a)M=\{0\}$．

提示：如果 $M=\langle m_1,\cdots,m_n\rangle$，则每个 $m_i=\sum_j a_{ij}m_j$，其中 $a_{ij}\in I$．和引理 11.41 的证明一样用伴随矩阵（余子式的矩阵）．

11.47 推广定理 9.8 的证明来证明如果 R 是左遗传环，则自由左 R-模 F 的每个子模同构于理想的直和，且因此是投射的．

11.48 设 R 是戴得金环，并设 $\mathfrak{p}$ 是 R 中的非零素理想．

（ⅰ）如果 $a\in\mathfrak{p}$，证明 $\mathfrak{p}$ 出现在 Ra 的素因子分解中．

（ⅱ）如果 $a\in\mathfrak{p}^e$ 和 $a\notin\mathfrak{p}^{e+1}$，证明 $\mathfrak{p}^e$ 出现在 Ra 的素因子分解中，但 $\mathfrak{p}^{e+1}$ 不出现在 Ra 的素因子分解中.

11.49 设 I 是戴得金环 R 中的非零理想．证明：如果 $\mathfrak{p}$ 是素理想，则 $I\subseteq\mathfrak{p}$ 当且仅当 $\mathfrak{p}$ 出现在 I 的素因子分解中．

11.50 如果 J 是戴得金环 R 的分式理想，证明对每个极大理想 $\mathfrak{p}$，$(J^{-1})_{\mathfrak{p}}=(J_{\mathfrak{p}})^{-1}$．

11.51 设 $I_1,\cdots,I_n$ 是戴得金环中的理想．如果存在非零素理想 $\mathfrak{p}$ 对一切 i 和理想 L_i 有 $I_i=\mathfrak{p}L_i$，则

$$I_1+\cdots+I_n=R.$$

11.52 举出一个不是自由的投射 $\mathbb{Z}[\sqrt{-5}]$-模的例子．

提示：见例 11.99.

11.53 （ⅰ）如果交换环 R 中的每个理想都是主理想，则称 R 为**主理想环**（如果 R 是整环，则 R 将是 PID）．例如 $\mathbb{I}_n$ 就是主理想环．证明 $\mathbb{Z}\times\mathbb{Z}$ 是主理想环．

（ⅱ）设 $I_1,\cdots,I_n$ 是交换环 R 中两两互素的理想．如果对每个 i，R/I_i 是主理想环．证明 $R/(I_1,\cdots,I_n)$ 是主理想环．

提示：用孙子剩余定理，即习题 6.11（ⅲ).

11.54 设 a 是戴得金环 R 中的非零元素．证明 R 中只有有限个理想 I 包含 a.

提示：如果 $a\in I$，则有某个理想 $I\subseteq R$ 使得 $Ra=IL$．

11.2.5 戴得金环上的有限生成模

在第 9 章中我们看到关于阿贝尔群的定理可以推广为关于 PID 上的模的定理，现在要把这些定理进一步推广到戴得金环上的模．

命题 11.103 设 R 是戴得金环．

（ⅰ）如果 $I\subseteq R$ 是非零理想，则 R/I 中的每个理想都是主理想．

（ⅱ）每个分式理想 J 都可由两个元素生成．更精确地说，对任一非零 $a\in J$，存在 $b\in J$ 使得 $J=Ra+Rb$．

证明 （i）设 $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$ 是 I 的素因子分解．因理想 $\mathfrak{p}_i^{e_i}$ 是两两互素的，根据习题11.53（ii），只需证明对每个 i，$R/\mathfrak{p}_i^{e_i}$ 是主理想环．现在 $R_{\mathfrak{p}_i} \otimes_R$ 的正合性表明 $(R/\mathfrak{p}_i^{e_i})_{\mathfrak{p}_i} \cong R_{\mathfrak{p}_i}/(\mathfrak{p}_i^{e_i})_{\mathfrak{p}_i}$．因 $R_{\mathfrak{p}_i}$ 是 PID（它甚至是 DVR），它的任意商环都是主理想环．

（ii）先假定 J 是整理想．选取非零 $a \in J$．根据（i），R/Ra 中的理想 J/Ra 是主理想；比如 J/Ra 由 $b + Ra$ 生成，其中 $b \in J$．由此，$J = Ra + Rb$．

关于一般情形，存在非零 $c \in R$ 使得 $cJ \subseteq R$（如果 J 是由 $u_1/v_1, \cdots, u_m/v_m$ 生成的，取 $c = \prod_j v_j$）．因 cJ 是整理想，给定任一非零 $a \in J$，存在 $cb \in cJ$ 使得 $cJ = Rca + Rcb$．因此 $J = Ra + Rb$．■

下一个系表明可以迫使非零理想互素．

系 11.104 *如果 I 和 J 都是戴得金环 R 上的分式理想，则存在 $a, b \in \mathrm{Frac}(R)$ 使得*

$$aI + bJ = R.$$

证明 选取非零 $a \in I^{-1}$．现在 $aI \subseteq I^{-1}I = R$，因此 $aIJ^{-1} \subseteq J^{-1}$．根据命题11.103（ii），存在 $b \in J^{-1}$ 使得

$$J^{-1} = aIJ^{-1} + Rb.$$

因 $b \in J^{-1}$，有 $bJ \subseteq R$，从而

$$R = JJ^{-1} = J(aIJ^{-1} + Rb) = aI + RbJ = aI + bJ.$$ ■

我们现在研究 R-模的结构．

引理 11.105 *设 R 是一个整环．*

（i）如果 $0 \to M' \to M \to M'' \to 0$ 是 R-模的短正合列，则

$$\mathrm{rank}(M) = \mathrm{rank}(M') + \mathrm{rank}(M'').$$

（ii）一个 R-模是挠的当且仅当 $\mathrm{rank}(M) = 0$．

（iii）如果 M 是有限生成无挠 R-模，且 $M \neq \{0\}$，则 $\mathrm{rank}(M) = 1$ 当且仅当 M 同构于一个非零理想．

证明 （i）根据系 8.103，分式域 F 是平坦 R-模．所以 $0 \to F \otimes_R M' \to F \otimes_R M \to F \otimes_R M'' \to 0$ 是 F 上的向量空间的短正合列，由此，本结果是线性代数中的常规结果（习题 3.74）．

（ii）如果 M 是挠的，则根据命题 8.95 的一个明显的推广，$F \otimes_R M = \{0\}$（可除的$\otimes$挠的 $= \{0\}$）．因此，$\mathrm{rank}(M) = 0$．反之，如果 $\mathrm{rank}(M) = 0$，则 $F \otimes_R M = \{0\}$．根据命题 11.25，如果 $S = R - \{0\}$ 和 $h_M : M \to S^{-1}M$ 是局部化映射，则 $\ker h_M = \{m \in M$：有某个 $\sigma \in R - \{0\}$ 使得 $\sigma m = 0\}$．于是 $M = \ker h_M$，因此 M 是挠的．

（iii）如果 $M \cong I$，其中 I 是理想，则 $\mathrm{rank}(M) = \mathrm{rank}(I)$，且存在正合列 $0 \to I \to F$．因 F 是平坦 R-模，序列 $0 \to F \otimes_R I \to F \otimes_R F$ 是正合的．但 $F \otimes_R F \cong F$ 的维数是 1，因此 $\mathrm{rank}(I) \leqslant 1$．由于 $I \neq \{0\}$（因为分式理想非零），因此有 $\mathrm{rank}(I) = 1$．

反之，假定 $\mathrm{rank}(M) = 1$；即 $F \otimes_R M \cong F$．选取非零元素 $u.\ v \in M$．如果 u，v 是线性无关的，则 $\langle u, v \rangle = \langle u \rangle \oplus \langle v \rangle$．但 $0 \to \langle u \rangle \oplus \langle v \rangle \to M$ 的正合性给出 $0 \to F \otimes_R \langle u \rangle \oplus_F \otimes_R \langle v \rangle \to F \otimes_R M$ 的正合性（再一次用到了 F 的平坦性）．这是一个矛盾，因为 1-维空间不可能有 2-维子空间．选取非零元素 $x \in M$．如果 $m \in M$，由上面的讨论可知存在非零 $r, s \in R$ 使得 $sm = rx$．读者可以修改定理 9.3 的证明用以证明由 $m \mapsto r/s$ 给出的函数 $M \to F$ 是 M 和 F 的一个子模 S 的合理定义的（因为 M 是无挠的）同构．由于 M 是有限生成的，所以 S 是分式理想．

剩下要证明每个分式理想 $J = \langle a_1/b_1, \cdots, a_n/b_n \rangle \subseteq F$ 同构于一个整理想．如果 $b = \prod_i b_i$，则对一切 $x \in J$，$bx \in R$，这是因为乘 b 只不过是清除分母．因此由 $x \mapsto bx$ 给出的映射 $J \to R$ 是R-映射；因为域没有零因子，所以它是单射． ■

命题 11.106 *如果 R 是戴得金环且 M 是有限生成无挠 R-模，则*

$$M \cong I_1 \oplus \cdots \oplus I_n,$$

其中 I_i 是 R 中的理想．

证明 对 $\operatorname{rank}(M) \geqslant 0$ 用归纳法证明．如果 $\operatorname{rank}(M) = 0$，根据引理11.105(ii)，$M$是挠的．因 M 是无挠的，所以 $M = \{0\}$．现在假定 $\operatorname{rank}(M) = n+1$．选取非零 $m \in M$，从而 $\operatorname{rank}(Rm) = 1$．序列

$$0 \to Rm \to M \xrightarrow{\nu} M'' \to 0$$

是正合的，其中 $M'' = R/Rm$ 和ν 是自然映射．注意，根据引理11.105(i)，$\operatorname{rank}(M'') = n$．现在是 M 有限生成的蕴涵M''也是有限生成的．如果 $T = t(M'')$ 是 M''的挠子模，则 M''/T 是有限生成的无挠 R-模，且 $\operatorname{rank}(M''/T) = \operatorname{rank}(M'') = n$，这是因为 $\operatorname{rank}(T) = 0$．根据归纳假设，$M''/T$ 是理想的直和，因此是投射的．定义

$$M' = \nu^{-1}(T) = \{m \in M : rm \in Rm, \text{对某个 } r \neq 0\} \subseteq M.$$

存在正合列 $0 \to M' \to M \to M''/T \to 0$；该序列分裂是因为 M''/T 是投射的；即 $M \cong M' \oplus (M''/T)$. 因此

$$\operatorname{rank}(M') = \operatorname{rank}(M) - \operatorname{rank}(M''/T) = 1.$$

因 R 是诺特环，所以有限生成 R-模的每个子模本身也都是有限生成的；因此 M' 是有限生成的．所以根据引理11.105(ii)，M' 同构于一个理想，证明完成． ■

系 11.107 *如果 R 是戴得金环且 M 是有限生成无挠 R-模，则 M 是投射的．*

证明 回忆一下，根据命题 11.98，戴得金环中的每个理想都是投射的．现在根据命题 11.106，M 是理想的直和，因此它是投射的．

也可以用局部化证明这个结果．对每个极大理想 $\mathfrak{m}$，$R_\mathfrak{m}$ -模 $M_\mathfrak{m}$ 是有限生成无挠的．然而，因 $R_\mathfrak{m}$ 是 PID（甚至是 DVR)，所以 $M_\mathfrak{m}$ 是自由模，因此它是投射的．现在从系 11.39 可得结果． ■

系 11.108 *如果 M 是有限生成 R-模，其中 R 是戴得金环，则挠子模 tM 是 M 的直和项．*

证明 商模 M/tM 是有限生成无挠 R-模，因此根据系 11.107，它是投射的．所以根据系 7.55，tM 是 M 的直和项． ■

系 11.109 *如果 R 是戴得金环，则每个无挠 R-模 A 是平坦的．*

证明 根据引理 8.97，只需证明 A 的每个有限生成子模是平坦的．但这样的子模是无挠的，因此是投射的，根据引理 8.98，投射模恒为平坦模． ■

可以证明在任意整环 R 上，每个平坦 R-模都是无挠的（见 Rotman 所著的《An Introduction to Homological Algebra》，129 页).

用同调代数可以去掉 tM 是有限生成的假设而推广系 11.108.

系 11.110 *设 R 是戴得金环且 $F = \operatorname{Frac}(R)$．*

(i) *如果 C 是无挠 R-模且 T 是挠模满足 $\operatorname{ann}(T) \neq \{0\}$，则 $\operatorname{Ext}^1_R(C, T) = \{0\}$．*

(ii) *设 M 是 R-模．如果 $\operatorname{ann}(tM) \neq \{0\}$，其中 tM 是 M 的挠子模，则 tM 是 M 的直和项．*

证明 (i) 我们推广命题 10.92 的证明．因 C是无挠的，根据系 11.109，它是平坦的，因此

$0 \to R \to F$ 的正合性给出 $0 \to R \otimes_R C \to F \otimes_R C$ 的正合性．于是 $C \cong R \otimes_R C$ 可以嵌入 F 上的一个向量空间 V，即 $V = F \otimes_R C$．运用反变函子 $\mathrm{Hom}_R(\ ,T)$ 到 $0 \to C \to V \to V/C \to 0$ 上得正合列

$$\mathrm{Ext}_R^1(V,T) \to \mathrm{Ext}_R^1(C,T) \to \mathrm{Ext}^2(V/C,T).$$

现在根据系 11.102，最后一项是 $\{0\}$，而根据例 10.70（它的一个简单推广），$\mathrm{Ext}_R^1(V,T)$ 是（无挠）可除的，因此 $\mathrm{Ext}_R^1(C,T)$ 是可除的．因 $\mathrm{ann}(T) \neq \{0\}$，习题 10.41 给出 $\mathrm{Ext}_R^1(C,T) = \{0\}$．

（ii）要证明扩张 $0 \to tM \to M \to M/tM \to 0$ 分裂，只需证明 $\mathrm{Ext}_R^1(M/tM, tM) = \{0\}$．因 M/tM 是无挠的，由（i）和系 10.90 可得该结论． ■

下一结果推广了命题 7.73.

命题 11.111 *对整环 R，下列陈述等价．*

（i）R 是戴得金环．

（ii）R-模 E 是内射的当且仅当它是可除的．

证明 （i）⇒（ii）．设 R 是戴得金环并设 E 是可除 R-模．根据白尔判别法，即定理 7.68，只需完成图



其中 I 是理想且 $i: I \to R$ 是包含映射．当然，可以假定 I 非零，因此 I 是可逆的：存在元素 $a_1, \cdots, a_n \in I$ 和元素 $q_1, \cdots, q_n \in F$ 使得 $q_i I \subseteq R$ 和 $1 = \sum_i q_i a_i$．因 E 是可除的，存在元素 $e_i \in E$ 使得 $f(a_i) = a_i e_i$．注意，对每个 $b \in I$，

$$f(b) = f\Big(\sum_i q_i a_i b\Big) = \sum_i (q_i b) f(a_i) = \sum_i (q_i b) a_i e_i = b \sum_i (q_i a_i) e_i.$$

因此，如果定义 $e = \sum_i (q_i a_i) e_i$，则 $e \in E$ 且对一切 $b \in I$，$f(b) = be$．定义 $g: R \to E$ 为 $g(r) = re$ 表明图可以完成，因此 E 是内射的．引理 7.72 中证明了每个内射 R-模是可除的．

（ii）⇒（i）．设 E 是内射 R-模．如果 E' 是 E 的商，则 E' 是可除的，因此根据假设它是内射的．内射模的每个商都是内射的，从而根据定理 11.101，R 是戴得金环． ■

考察了无挠模后，现在我们来看挠模．

命题 11.112 *设 $\mathfrak{p}$ 是戴得金环中的非零素理想．如果 M 是 R-模，且有某个 $e > 0$ 使得 $\mathrm{ann}(M) = \mathfrak{p}^e$，则局部化映射 $M \to M_\mathfrak{p}$ 是同构（因此可把 M 看作 $R_\mathfrak{p}$-模）．*

证明 只需证明 $M \cong R_\mathfrak{p} \otimes_R M$．如果 $m \in M$ 非零且 $s \in R$ 满足 $s \notin \mathfrak{p}$，则根据命题 11.97 有

$$\mathfrak{p}^e + Rs = R,$$

因此存在 $u \in \mathfrak{p}^e$ 和 $r \in R$ 使得 $1 = u + rs$，从而

$$m = um + rsm = rsm.$$

如果 $1 = u' + r's$，其中 $u' \in \mathfrak{p}$ 和 $r' \in R$，则 $s(r - r')m = 0$，从而

$$s(r - r') \in \mathrm{ann}(m) = \mathfrak{p}^e.$$

因 $s \notin \mathfrak{p}^e$，所以 $r - r' \in \mathfrak{p}^e$（$Rs$ 的素因子分解不包含 $\mathfrak{p}^e$；如果 $R(r-r')$ 的素因子分解不包含 $\mathfrak{p}^e$，则 $Rs(r-r')$ 的素因子分解也不包含 $\mathfrak{p}^e$）．因此，$rm = r'm$．定义 $s^{-1}m = rm$．定义 $f: R_\mathfrak{p} \times M \to M$ 为 $f(r/s, m) = s^{-1}rm$，其中 $s^{-1}rm$ 已在前段定义．容易验证 f 是 R-双线性的，因此存在 R-映射

$\tilde{f}: R_\mathfrak{p} \otimes M \to M$ 使得 $\tilde{f}(r/s \otimes m) = s^{-1}rm$．特别地，$\tilde{f}(1 \otimes m) = m$，因此 f 是满射．另一方面，易知由 $h_M(m) = 1 \otimes m$ 定义的局部化映射 $h_M: M \to R_\mathfrak{p} \otimes_R M$ 是$\tilde{f}$ 的逆． ■

定义 设 $\mathfrak{p}$ 是戴得金环 R 中的非零素理想．如果一个 R-模 M 满足对每个 $m \in M$ 有 $e > 0$ 使得 $\text{ann}(m) = \mathfrak{p}^e$，则称 M 为 $\mathfrak{p}$-**准素的**．

定理 11.113（准素分解） 设 R 是戴得金环，并设 T 是有限生成挠 R-模．如果 $I = \text{ann}(T) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$，则

$$T = T[\mathfrak{p}_1] \oplus \cdots \oplus T[\mathfrak{p}_n],$$

其中

$$T[\mathfrak{p}_i] = \{m \in T: \text{ann}(m) \text{ 是 } \mathfrak{p}_i \text{ 的幂}\}.$$

$T[\mathfrak{p}_i]$ 叫做 T 的 $\mathfrak{p}_i$-**准素分量**．

证明 易知 $\mathfrak{p}_i$-准素分量 $T[\mathfrak{p}_i]$ 是 T 的子模．现在验证命题 7.19 中的条件．如果 W_i 是由 $j \neq i$ 的一切 $T[\mathfrak{p}_j]$ 生成的 T 的子模，我们需要证明 $T[\mathfrak{p}_i] \cap W_i = \{0\}$．设 $x \in T[\mathfrak{p}_i] \cap W_i$．如果

$$I_i = \mathfrak{p}_1^{e_1} \cdots \hat{\mathfrak{p}}_i^{e_i} \cdots \mathfrak{p}_n^{e_n},$$

则 $\mathfrak{p}_i$ 和 I_i 互素：$\mathfrak{p}_i + I_i = R$．因此存在 $a_i \in \mathfrak{p}_i$ 和 $r_i \in I_i$ 使得 $1 = a_i + r_i$，从而 $x = a_i x + r_i x$．但因 $x \in T[\mathfrak{p}_i]$，因此 $a_i x = 0$，又因 $x \in W_i$ 且 $I_i = \text{ann}(W_i)$，因此 $r_i x = 0$．所以 $x = 0$．

根据习题 11.51，有

$$I_1 + \cdots + I_n = R.$$

于是，存在 $b_i \in I_i$ 使得 $b_1 + \cdots + b_n = 1$．如果 $t \in T$，则 $t = b_1 t + \cdots + b_n t$．但如果 $c_i \in \mathfrak{p}_i^{e_i}$，则 $c_i b_i \in \mathfrak{p}_i^{e_i} I_i = I = \text{ann}(T)$，从而 $c_i(b_i t) = 0$．因此 $\mathfrak{p}_i^{e_i} \subseteq \text{ann}(b_i t)$，于是有某个 $e > 0$ 使得 $\text{ann}(b_i t) = \mathfrak{p}_i^{e}$．所以 $b_i t \in T[\mathfrak{p}_i]$，因此

$$T = T[\mathfrak{p}_1] + \cdots + T[\mathfrak{p}_n].$$

现在由命题 7.19 可得结果． ■

定理 11.114 设 R 是戴得金环．

（i）两个有限生成挠 R-模 T 和 T' 同构当且仅当对一切 i，$T[\mathfrak{p}_i] \cong T'[\mathfrak{p}_i]$．

（ii）每个有限生成 $\mathfrak{p}$-准素 R-模 T 都是循环 R-模的直和，且每个类型的直和项个数是 T 的不变量．

证明 （i）只需看到如果 $f: T \to T'$ 是同构，则对一切 $t \in T$ 有 $\text{ann}(t) = \text{ann}(f(t))$ 就可得到结果.

（ii）准素分解表明 T 是它的准素分量 $T[\mathfrak{p}_i]$ 的直和．根据命题 11.112，$T[\mathfrak{p}_i]$ 是 $R_{\mathfrak{p}_i}$-模．但 $R_{\mathfrak{p}_i}$ 是 PID（甚至是 DVR），因此基定理和基本定理成立：每个 $T[\mathfrak{p}_i]$ 是循环模的直和，且循环直和项的同构的类型个数是唯一确定的． ■

我们现在知道每个有限生成 R-模 M 都是循环模和理想的直和．这种分解有怎样的唯一性？因挠子模是一个完全不变的直和项，我们可以专注于无挠模．

回忆命题 11.3：整环 R 中的两个理想 J 和 J' 同构当且仅当存在 $a \in \text{Frac}(R)$ 使得 $J' = aJ$．

引理 11.115 设 M 是有限生成无挠 R-模，其中 R 是戴得金环，因此 $M \cong I_1 \oplus \cdots \oplus I_n$，其中 I_i 是理想．则

$$M \cong R^{n-1} \oplus J,$$

其中 $J = I_1 \cdots I_n$．

注 称 $R^{n-1} \oplus J$ 为 M 的**施泰尼茨正规型**．在定理 11.117 中将证明不计同构 J 是唯一的．

证明　只需证明 $I\oplus J\cong R\oplus IJ$，因为容易对 $n\geqslant 2$ 用归纳法得到结果．根据系 11.104，存在非零 $a,b\in \mathrm{Frac}(R)$ 使得 $aI+bJ=R$．因 $aI\cong I$ 和 $bJ\cong J$，我们可以假定 I 和 J 是互素的整理想．存在正合列

$$0\to I\cap J\xrightarrow{\delta} I\oplus J\xrightarrow{\alpha} I+J\to 0,$$

其中 $\delta: x\mapsto (x,x)$ 和 $\sigma: (u,v)\mapsto u-v$．然而，因 I 和 J 是互素的，有 $I\cap J=IJ$ 和 $I+J=R$．由于 R 是投射的，这个序列分裂；即 $I\oplus J\cong R\oplus IJ$． ■

下面的消去引理对戴得金环成立，但对某些其他环不成立．在例 7.78（ⅲ）中我们描述了 Swan 的一个例子，它表明如果 $R=\mathbb{R}[x_1,\cdots,x_n]/\left(1-\sum_i x_i^2\right)$ 是 3-球面的实坐标环，则存在不是自由的有限生成稳定自由 R-模 M. 因此存在自由 R-模 F 和 F' 满足 $M\oplus F\cong F'\oplus F$，但 $M\not\cong F'$.

引理 11.116　*设 R 是戴得金环．如果 $R\oplus G\cong R\oplus H$，其中 G 和 H 都是 R-模，则 $G\cong H$.*

证明　可以假定存在模 $E=A\oplus G=B\oplus H$，其中 $A\cong R\cong B$．设 $p: E\to B$ 是投射 $p:(b,h)\mapsto b$，并设 $p'=p\mid G$．现在

$$\ker p'=G\cap H \quad 和 \quad \mathrm{im}\, p'\subseteq B\cong R.$$

于是 $\mathrm{im}\, p'\cong L$，其中 L 是 R 中的一个理想．

如果 $\mathrm{im}\, p'=\{0\}$，则 $G\subseteq \ker p=H$．因 $E=A\oplus G$，系 7.18 给出 $H=G\oplus(H\cap A)$．一方面，$E/G=(A\oplus G)/G\cong A\cong R$；另一方面，$E/G=(B\oplus H)/G\cong B\oplus(H/G)\cong R\oplus(H/G)$．于是，$R\cong R\oplus(H/G)$．因 R 是整环，这就迫使 $H/G=\{0\}$；如果 $R=X\oplus Y$，则 X 和 Y 都是理想；如果 $x\in X$ 和 $y\in Y$ 都非零，则 $xy\in X\cap Y=\{0\}$，这给出 R 中的零因子．由此，$H/G=\{0\}$ 和 $G=H$.

现在可以假定 $L=\mathrm{im}\, p'$ 是非零理想．第一同构定理给出 $G/(G\cap H)\cong L$．因 R 是戴得金环，L 是投射模，所以

$$G=I\oplus(G\cap H),$$

其中 $I\cong L$．类似地，

$$H=J\oplus(G\cap H),$$

其中 J 同构于一个理想．由此

$$E=A\oplus G=A\oplus I\oplus(G\cap H);$$
$$E=B\oplus H=B\oplus J\oplus(G\cap H).$$

从而

$$A\oplus I\cong E/(G\cap H)\cong B\oplus J.$$

如果能够证明 $I\cong J$，则

$$G=I\oplus(G\cap H)\cong J\oplus(G\cap H)=H.$$

因此，我们已经把定理化简为 G 和 H 都是非零理想的特殊情形．

我们将证明如果 $\alpha: R\oplus I\to R\oplus J$ 是同构，则 $I\cong J$．和在 540 页讨论广义矩阵一样，α 确定了一个 2×2 矩阵

$$A=\begin{bmatrix} a_{11} & a_{12}\\ a_{21} & a_{22}\end{bmatrix},$$

其中 $a_{11}:R\to R$，$a_{21}:R\to J$，$a_{12}:I\to R$，$a_{22}:I\to J$．事实上，理想之间的映射就是乘以 $F=\mathrm{Frac}(R)$ 的一个元素，从而可以把 A 看作 $\mathrm{GL}(2,F)$ 中的矩阵．现在 $a_{21}\in J$ 和 $a_{22}I\subseteq J$，因此，如果 $d=\det(A)$，则

$$dI=(a_{11}a_{22}-a_{12}a_{12})I\subseteq J.$$

类似地，$\beta=\alpha^{-1}$ 确定一个 2×2 矩阵 $B=A^{-1}$．

$$d^{-1}J=\det(B)J\subseteq I,$$

因此 $J\subseteq dI$．由此可知 $J=dI$，从而 $J\cong I$． ■

我们用外代数概要证明如果 R 是戴得金环且 I,J 都是分式理想，则 $R\oplus I\cong R\oplus J$ 蕴涵 $I\cong J$．原始证明中运用 2×2 行列式的事实说明二次外幂可能有用．根据定理 9.143，

$$\bigwedge^2(R\oplus I)\cong\left(R\otimes\bigwedge^2(I)\right)\oplus\left(\bigwedge^1(R)\otimes_R\bigwedge^1(I)\right)\oplus\left(\bigwedge^2(R)\otimes_R I\right).$$

现在根据系 9.138，$\bigwedge^2(R)=\{0\}$，$\bigwedge^1(R)\otimes_R\bigwedge^1(I)\cong R\otimes_R I\cong I$．我们现在证明对每个极大理想 $\mathfrak{m}$，$(\bigwedge^2(I)_{\mathfrak{m}}=\{0\})$．根据习题 11.24，

$$\left(\bigwedge^n(I)\right)_{\mathfrak{m}}\cong\bigwedge^n(I_{\mathfrak{m}}).$$

但 $R_{\mathfrak{m}}$ 是 PID，从而 $I_{\mathfrak{m}}$ 是主理想，因此根据系 9.138，$\bigwedge^2(I_{\mathfrak{m}})=\{0\}$．所以 $\bigwedge^2(R\oplus I)\cong I$．类似地，$\bigwedge^2(R\oplus J)\cong J$，因此 $I\cong J$．

定理 11.117（施泰尼茨） *设 R 是戴得金环，并设 $M\cong I_1\oplus\cdots\oplus I_n$ 和 $M'\cong I'_1\oplus\cdots\oplus I'_\ell$ 都是有限生成无挠 R-模，则 $M\cong M'$ 当且仅当 $n=\ell$ 且 $I_1\cdots I_n\cong I'_1\cdots I'_n$．*

证明 引理11.105(ⅲ)表明对一切 i，$\mathrm{rank}(I_i)=1$，引理11.105(ⅰ)表明 $\mathrm{rank}(M)=n$；类似地，$\mathrm{rank}(M')=\ell$．因 $M\cong M'$，有 $F\otimes_R M\cong F\otimes_R M'$，从而 $\mathrm{rank}(M)=\mathrm{rank}(M')$ 和 $n=\ell$. 根据引理 11.115，只需证明如果 $R^n\oplus I\cong R^n\oplus J$，则 $I\cong J$．但重复运用引理 11.116 立刻得到此结果． ■

设 R 是交换环，并设$\mathcal{C}$是 ${}_R\mathbf{Mod}$ 的子范畴．回忆两个 R-模 A 和 B 称为在$\mathcal{C}$中稳定同构，如果存在模 $C\in\mathrm{obj}(\mathcal{C})$ 使得 $A\oplus C\cong B\oplus C$．

系 11.118 *设 R 是戴得金环，并设$\mathcal{C}$是一切有限生成无挠 R-模的范畴．则 $M,M'\in\mathcal{C}$ 在$\mathcal{C}$中稳定同构当且仅当它们同构．*

证明 同构模恒稳定同构．为证明逆命题，假定存在有限生成无挠 R-模 X 使得

$$M\oplus X\cong M'\oplus X.$$

存在理想 I,J,L 使得 $M\cong R^{n-1}\oplus I$，$M'\cong R^{n-1}\oplus J$ 和 $X\cong R^{m-1}\oplus L$，其中 $n=\mathrm{rank}(M)=\mathrm{rank}(M')$．因此，

$$M\oplus X\cong R^{n-1}\oplus I\oplus R^{m-1}\oplus L\cong R^{n+m-1}\oplus IL.$$

类似地，

$$M'\oplus X\cong R^{n+m-1}\oplus JL.$$

根据定理 11.117，$IL\cong JL$，从而根据引理 11.3，存在非零 $a\in\mathrm{Frac}(R)$ 使得 $aIL=JL$．乘以 L^{-1} 得$aI=J$，因此$I\cong J$．所以，

$$M\cong R^{n-1}\oplus I\cong R^{n-1}\oplus J\cong M'.$$ ■

回忆一下，如果范畴$\mathcal{C}$有有限积，则格罗滕迪克群 $K_0(\mathcal{C})$ 是这样的阿贝尔群，它的生成元为

obj($\mathcal{C}$)（的同构类），关系为对一切 $A,B\in$obj($\mathcal{C}$)，$A\oplus B=A+B$；即 $K_0(\mathcal{C})=\mathcal{F}(\mathcal{C})/\mathcal{R}$，其中 $\mathcal{F}(\mathcal{C})$ 是以 obj($\mathcal{C}$) 为基的自由阿贝尔群，$\mathcal{R}$是由一切 $A\oplus B-A-B$ 生成的子群．如果以 $[A]$ 表示 $K_0(\mathcal{C})$ 中的元素 $A+\mathcal{R}$，其中 $A\in$obj($\mathcal{C}$)，则根据命题 7.77，在 $K_0(\mathcal{C})$ 中 $[A]=[B]$ 当且仅当它们在$\mathcal{C}$中稳定同构．

记号　如果 $\mathbf{Pr}(R)$ 是交换环 R 上一切有限生成投射 R-模的范畴，则记

$$K_0(R)=K_0(\mathbf{Pr}(R)).$$

在结束本节的时候，我们展示戴得金环 R 的类群 $C(R)$ 和它的格罗滕迪克群 $K_0(R)$ 之间的关系．如果 I 是戴得金环 R 中的非零理想，则记 $C(R)$ 中对应的元素为 cls(I)．

定理 11.119　如果 R 是戴得金环，则

$$K_0(R)\cong C(R)\oplus \mathbf{Z},$$

其中 $C(R)$ 是 R 的类群．

证明　如果 P 是有限生成投射 R-模，根据引理 11.115，有非零理想 I 使得 $P\cong R^{n-1}\oplus I$；此外，根据定理 11.117，I 的同构类是由 P 唯一确定的．如果 $P\cong R^{n-1}\oplus J$，则存在 $a\in\mathrm{Frac}(R)$ 使得$J=aI$，从而在 $C(R)$ 中有 $\mathrm{cls}(J)=\mathrm{cls}(I)$．所以由

$$\varphi([P])=(\mathrm{cls}(I),\mathrm{rank}(P))$$

给出的函数 $\varphi:K_0(R)\to C(R)\oplus\mathbf{Z}$ 是合理定义的．注意，我们把第一个直和项 $C(R)$ 写作乘性的，而把第二个直和项 $\mathbf{Z}$ 写作加性的．为证明 φ 在 $K_0(R)=\mathcal{F}(\mathbf{Pr}(R))/\mathcal{R}$ 上是合理定义的，只需证明它保持$\mathcal{R}$中的关系；即

$$\varphi([P\oplus Q])-\varphi([P])-\varphi([Q])=0.$$

设 $Q=R^{m-1}\oplus J$，其中 J 是非零理想．则 $P\oplus Q\cong R^{n+m-1}\oplus IJ$，且

$$\begin{aligned}\varphi([P\oplus Q])&=(\mathrm{cls}(IJ),n+m)\\&=(\mathrm{cls}(I)\mathrm{cls}(J),n+m)\\&=(\mathrm{cls}(I),n)+(\mathrm{cls}(J),m).\end{aligned}$$

因 $\mathrm{rank}(P\oplus Q)=\mathrm{rank}(P)+\mathrm{rank}(Q)$，从而 φ 是合理定义的同态．

现在因为 $(\mathrm{cls}(I),n)=\varphi([R^{n-1}\oplus I])$，且 $C(R)\oplus\mathbf{Z}$ 是由一切这样的元素生成的，所以 φ 是满射．为证明 φ 是单射，回忆命题 7.77 表明 $K_0(R)$ 的典型元素形如 $[P]-[Q]$．如果 $\varphi([P]-[Q])=0$，则 $\varphi([P])=\varphi([Q])$．因此命题 7.77 表明 P 和 Q 稳定同构．系 11.118 表明 $P\cong Q$，从而 $[P]-[Q]=0$．所以 φ 是同构．■

注　在这个背景中还有另外的格罗滕迪克群．一个 R-模 A 叫做**可逆的**，如果它是有限生成的，且 $A\otimes_R\mathrm{Hom}_R(A,R)\cong R$．根据命题 8.83 和 9.97，一切可逆 R-模的范畴在张量积下是一个★-范畴，因此它有格罗滕迪克群，这个群叫做**皮卡群**，记为 Pic(R)．由此得出每个可逆模和一个理想同构．于是，Pic(R) 是阿贝尔群（写作乘性的），它的生成元是 R 中的一切可逆理想，关系是 $I\otimes_R J=IJ$．当 R 是戴得金环时，$\mathrm{Pic}(R)\cong C(R)$．

习题

11.55　设 R 是戴得金环，并设 $I\subseteq R$ 是非零理想．证明存在理想 $J\subseteq R$ 使得 $I+J=R$ 且 IJ 是主理想．

提示：设 $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$，并选取 $r_i \in \mathfrak{p}_i^{e_i} - \mathfrak{p}_i^{e_i+1}$．用孙子剩余定理求出元素 $a \in R$ 使得 $a \in \mathfrak{p}_i^{e_i}$ 和 $a \notin \mathfrak{p}_i^{e_i+1}$，并考虑 Ra 的素因子分解．

11.56 (i) 如果 R 是交换环，证明 $R^n \cong R^m$ 蕴涵 $n = m$．

提示：如果 $\mathfrak{m}$ 是 R 中的极大理想，则 $(R/\mathfrak{m})$-向量空间 $(R/\mathfrak{m})^n$ 和 $(R/\mathfrak{m})^m$ 同构．

(ii) 如果 R 是任意交换环，证明$\mathbb{Z}$ 是 $K_0(R)$ 的直和项．

11.57 如果 R 是 PID，证明 $K_0(R) \cong \mathbb{Z}$．

11.58 如果 I 是戴得金环 R 中的分式理想，证明 $I \otimes I^{-1} \cong R$．

提示：用 I 的可逆性．

11.59 如果 R 是局部环，证明 $K_0(R) \cong \mathbb{Z}$．

11.60 如果 R 是交换环，证明秩定义了一个满同态 $K_0(R) \to \mathbb{Z}$．我们通常称这个映射的核为约化格罗滕迪克群，并记为 $\widetilde{K}_0(R)$．因此，

$$K_0(R) \cong \widetilde{K}_0(R) \oplus \mathbb{Z}.$$

11.61 如果$\mathcal{C}$是 ${}_R\mathbf{Mod}$ 的子范畴，则在 492 页上我们定义了格罗滕迪克群的一个变种：$K'(\mathcal{C})$ 是阿贝尔群，它的生成元是 $\mathrm{obj}(\mathcal{C})$，关系是 $B = A - C$，如果存在（不必分裂）正合列 $0 \to A \to B \to C \to 0$．

(i) 如果 R 是戴得金环，证明命题 7.82 的同态 $\varepsilon: K_0(R) \to K'(\mathcal{C})$ 的限制是同构 $\widetilde{K}_0(R) \to K'(\mathcal{C})$．

(ii) 如果 R 是戴得金环，证明 $K'(\mathcal{C}) \cong C(R)$．

11.3 整体维数

有几个类型的环，对它们的有限生成模已经作了分类：半单环；PID；戴得金环．这些环中的每一个都能用它的投射模来刻画：环 R 是半单的当且仅当每个 R-模是投射的；整环 R 是戴得金环当且仅当每个理想是投射的．整体维数的概念使得我们可以对任意环进行分类．

本节中的环不必是交换的．

定义 *设 R 是环并设 A 是左 R-模．如果存在有限投射分解*

$$0 \to P_n \to \cdots \to P_1 \to P_0 \to A \to 0,$$

*则记为 $pd(A) \leqslant n$．如果 $n \geqslant 0$ 是使得 $pd(A) \leqslant n$ 的最小整数，则我们说 A 有***投射维数** *n；如果不存在 A 的有限投射分解，则 $pd(A) = \infty$．*

例 11.120 (i) 模 A 是投射的当且仅当 $pd(A) = 0$．于是可以把 $pd(A)$ 看作 A 离开投射的程度的测度．

(ii) 如果 R 是戴得金环，则对每个 R-模 A，$pd(A) \leqslant 1$．根据定理 11.101，自由 R-模的每个子模都是投射的．因此，如果 F 是自由 R-模且 $\varepsilon: F \to A$ 是满射，则

$$0 \to \ker\varepsilon \to F \xrightarrow{\varepsilon} A \to 0$$

是 A 的投射分解．这个论证可以推广到左遗传环上． ■

定义 *设 $\mathbf{P}_\bullet = \cdots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} A \to 0$ 是模 A 的投射分解．如果 $n \geqslant 0$，则 n 次合冲是指*

$$\Omega_n(A, \mathbf{P}_\bullet) = \begin{cases} \ker\varepsilon & \text{如果 } n = 0 \\ \ker d_n & \text{如果 } n \geqslant 1. \end{cases}$$

命题 11.121 *对每个 $n \geqslant 1$，对一切左 R-模 A 和 B 以及 B 的每个投射分解 $\mathbf{P}_\bullet$，存在同构*

$$\mathrm{Ext}_R^{n+1}(A, B) \cong \mathrm{Ext}_R^1(\Omega_{n-1}(A, \mathbf{P}_\bullet), B).$$

证明 对 $n \geqslant 1$ 用归纳法证明. 投射分解

$$\mathbf{P}_{\bullet} = \cdots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} A \to 0$$

的正合性给出

$$\cdots \to P_2 \xrightarrow{d_2} P_1 \to \Omega_0(A, \mathbf{P}_{\bullet}) \to 0$$

的正合性，它是 $\Omega_0(A, \mathbf{P}_{\bullet})$ 的投射分解 $\mathbf{P}_{\bullet}^{+}$. 详细地说，定义

$$P_n^{+} = P_{n+1} \text{ 和 } d_n^{+} = d_{n+1}.$$

因 Ext^1 不依赖于第一个变量的投射分解的选取，所以

$$\mathrm{Ext}_R^1(\Omega_0(A, \mathbf{P}_{\bullet}), B) = \frac{\ker(d_2^{+})^*}{\mathrm{im}(d_1^{+})^*} = \frac{\ker(d_3)^*}{\mathrm{im}(d_2)^*} = \mathrm{Ext}_R^2(A, B).$$

归纳步用同样的方法证明，注意

$$\cdots \to P_{n+2} \xrightarrow{d_{n+2}} P_{n+1} \to \Omega_n(A, \mathbf{P}_{\bullet}) \to 0$$

是 $\Omega_n(A, \mathbf{P}_{\bullet})$ 的投射分解. ■

系 11.122 *对一切左 R-模 A 和 B，对一切 $n \geqslant 0$ 及 A 的任意投射分解 $\mathbf{P}_{\bullet}$ 和 $\mathbf{P}'_{\bullet}$，存在同构*

$$\mathrm{Ext}_R^1(\Omega_n(A, \mathbf{P}_{\bullet}), B) \cong \mathrm{Ext}_R^1(\Omega_n(A, \mathbf{P}'_{\bullet}), B).$$

证明 根据命题 11.121，两者都同构于 $\mathrm{Ext}_R^{n+1}(A, B)$. ■

如果对两个模 Ω 和 Ω' 存在投射模 P 和 P' 使得 $\Omega \oplus P \cong \Omega' \oplus P'$，则称 Ω 和 Ω' 是**投射等价的**. 习题 11.62 证明模 A 的任意两个 n 次合冲是投射等价的. 我们常泛用记号并说一个模的 n 次合冲，并写作 $\Omega_n(A)$ 来代替 $\Omega_n(A, \mathbf{P}_{\bullet})$.

合冲有助于投射维数的计算.

引理 11.123 *对左 R-模 A 下列条件等价*:

(i) $pd(A) \leqslant n$.

(ii) *对一切模 B 和一切 $k \geqslant n+1$，$\mathrm{Ext}_R^k(A, B) = \{0\}$.*

(iii) *对一切模 B，$\mathrm{Ext}_R^{n+1}(A, B) = \{0\}$.*

(iv) *对 A 的每个投射分解 $\mathbf{P}_{\bullet}$，$(n-1)$ 次合冲 $\Omega_{n-1}(A, \mathbf{P}_{\bullet})$ 是投射的.*

(v) *存在 A 的投射分解 $\mathbf{P}_{\bullet}$ 使得 $\Omega_{n-1}(A, \mathbf{P}_{\bullet})$ 是投射的.*

证明 (i) ⇒ (ii). 根据假设，存在 A 的投射分解 $\mathbf{P}_{\bullet}$ 使得对一切 $k \geqslant n+1$，$P_k = \{0\}$. 对 $k \geqslant n+1$，必然有一切映射 $d_k : P_k \to P_{k-1}$ 都是零. 因此

$$\mathrm{Ext}_R^k(A, B) = \frac{\ker(d_{k+1})^*}{\mathrm{im}(d_k)^*} = \{0\}.$$

(ii) ⇒ (iii). 显然成立.

(iii) ⇒ (iv). 如果 $\mathbf{P}_{\bullet} = \cdots \to P_n \to P_{n-1} \to \cdots \to P_1 \to P_0 \to A \to 0$ 是 A 的投射分解，则根据命题 11.121，$\mathrm{Ext}_R^{n+1}(A, B) \cong \mathrm{Ext}_R^1(\Omega_{n-1}(A, \mathbf{P}_{\bullet}), B)$. 但根据假设，最后一个群是 $\{0\}$，从而根据系 10.86，$\Omega_{n-1}(A)$ 是投射的.

(iv) ⇒ (v). 显然成立.

(v) ⇒ (i). 如果

$$\cdots \to P_n \to P_{n-1} \to \cdots \to P_1 \to P_0 \to A \to 0$$

是 A 的投射分解，则

$$0 \to \Omega_{n-1}(A) \to P_{n-1} \to \cdots \to P_1 \to P_0 \to A \to 0$$

是正合列．因 $\Omega_{n-1}(A)$ 是投射的，上面的序列是 A 的投射分解，因此 $pd(A) \leqslant n$． ■

例 11.124 设 G 是有限循环群且 $|G|>1$．如果把 $\mathbb{Z}$ 看作平凡 $\mathbb{Z}G$-模，则 $pd(\mathbb{Z})=\infty$，这是因为系 10.108 对一切奇数 n 给出

$$H^n(G,\mathbb{Z}) = \mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z},\mathbb{Z}) \neq \{0\}.$$ ■

下面的定义立刻可以简化．

定义 如果 R 是环，则它的**左投射整体维数**定义为

$$lpD(R) = \sup\{pd(A) : A \in \mathrm{obj}({}_R\mathbf{Mod})\}.$$

命题 11.125 对任意环 R，

$lpD(R) \leqslant n$ 当且仅当对一切左 R-模 A 和 B 有 $\mathrm{Ext}^{n+1}_R(A,B)=\{0\}$.

证明 从引理 11.123 中（ⅰ）和（ⅲ）的等价性立即可得． ■

例 11.126 （ⅰ）环 R 是半单的当且仅当 $lpD(R)=0$．于是，整体维数测量了一个环离开半单性的程度．

（ⅱ）环 R 是左遗传的当且仅当 $lpD(R) \leqslant 1$．特别地，整环 R 是戴得金环当且仅当 $pD(R) \leqslant 1$. ■

用内射分解可以给出类似的讨论．

定义 设 R 是环并设 B 是左 R-模．如果存在内射分解

$$0 \to B \to E^0 \to E^1 \to \cdots \to E^n \to 0,$$

则记 $id(B) \leqslant n$．如果 $n \geqslant 0$ 是使得 $id(B) \leqslant n$ 的最小整数，则我们说 B 有**内射维数** n；如果不存在 B 的有限内射分解，则 $id(B)=\infty$.

例 11.127 （ⅰ）模 B 是内射的当且仅当 $id(B)=0$．于是可以认为 $id(B)$ 测量了 B 离开内射性的程度．

（ⅱ）模 A 的内射和投射维数可以不同．例如阿贝尔群 $A=\mathbb{Z}$ 有 $pd(A)=0$ 和 $id(A)=1$．

（ⅲ）如果 R 是戴得金环，则定理 11.101 说内射 R-模的每个商模是内射的．因此，如果 $\eta: B \to E$ 是 R-模 B 到内射 R-模 E 的嵌入，则

$$0 \to B \xrightarrow{\eta} E \to \mathrm{coker}\,\eta \to 0$$

是 B 的内射分解．由此 $id(B) \leqslant 1$． ■

定义 设 $\mathbf{E}^\bullet = 0 \to B \xrightarrow{\eta} E^0 \xrightarrow{d^0} E^1 \xrightarrow{d^1} E^2 \to \cdots$ 是模 B 的内射分解．如果 $n \geqslant 0$，则 n 次上合冲是指

$$\mho^n(B,\mathbf{E}^\bullet) = \begin{cases} \mathrm{coker}\,\eta & \text{如果 } n=0 \\ \mathrm{coker} d^{n-1} & \text{如果 } n \geqslant 1. \end{cases}$$

命题 11.128 对每个 $n \geqslant 1$，对一切左 R-模 A 和 B 以及 A 的每个内射分解 $\mathbf{E}^\bullet$，存在同构

$$\mathrm{Ext}^{n+1}_R(A,B) \cong \mathrm{Ext}^1_R(A,\mho^{n-1}(B,\mathbf{E}^\bullet)).$$

证明 命题 11.121 证明的对偶． ■

系 11.129 对一切左 R-模 A 和 B，对一切 $n \geqslant 0$，以及对 B 的任意内射分解 $\mathbf{E}^\bullet$ 和 $\mathbf{E}'^\bullet$，存在同构

$$\mathrm{Ext}^1_R(A,\mho^n(B,\mathbf{E}^\bullet)) \cong \mathrm{Ext}^1_R(A,\mho^n(B,\mathbf{E}'^\bullet)).$$

证明 系 11.122 证明的对偶． ■

如果对两个模 U和 U' 存在内射模 E 和 E' 使得 $U \oplus E \cong U' \oplus E'$，则称 U和 U' **内射等价**．习题 11.63 证明模 B 的任意两个 n 次上合冲内射等价．我们常泛用记号并说一个模的 n 次上合冲，写作 $U^n(B)$ 代替 $U^n(B,\mathbf{E}^\bullet)$．

上合冲有助于内射维数的计算．

引理 11.130 对左 R-模 B 下列条件等价．

（i）$id(B) \leqslant n$．

（ii）对一切模 A 和一切 $k \geqslant n+1$，$\mathrm{Ext}_R^k(A,B)=\{0\}$．

（iii）对一切模 A，$\mathrm{Ext}_R^{n+1}(A,B)=\{0\}$．

（iv）对 B 的每个内射分解 $\mathbf{E}^\bullet$，$(n-1)$ 次上合冲 $U^{n-1}(B,\mathbf{E}^\bullet)$ 是内射的．

（v）存在 B 的内射分解 $\mathbf{E}^\bullet$ 使得 $U^{n-1}(B,\mathbf{E}^\bullet)$ 是内射的．

证明 引理 11.123 证明的对偶，用习题 10.49． ■

定义 如果 R 是环，则**左内射整体维数**定义为

$$liD(R)=\sup\{id(B): B \in \mathrm{obj}({}_R\mathbf{Mod})\}.$$

命题 11.131 对任意环 R，

$$liD(R) \leqslant n \text{ 当且仅当对一切左 } R\text{-模 } A \text{ 和 } B \text{ 有 } \mathrm{Ext}_R^{n+1}(A,B)=\{0\}.$$

证明 从引理 11.130 中的（i）和（iii）等价立得． ■

定理 11.132 对每个环 R，

$$lpD(R)=liD(R).$$

证明 从命题 11.125 和命题 11.131 立得，因为这两个数都等于这样的数：对一切左 R-模 A 和 B 满足 $\mathrm{Ext}_R^{n+1}(A,B)=\{0\}$ 的最小 n． ■

定义 环 R 的**左整体维数**是指左投射整体维数和左内射整体维数的公共值：

$$lD(R)=lpD(R)=liD(R).$$

如果 R 是交换环，则记它的整体维数为 $D(R)$．

还有环 R 的**右整体维数** $rD(R)=lD(R^{\mathrm{op}})$．如果 R 是交换的，则 $lD(R)=rD(R)$，并记为 $D(R)$．根据系 8.57，因左半单环也是右半单环，从而有 $lD(R)=0$ 当且仅当 $rD(R)=0$．另一方面，有环的例子，其中两个维数不同．

现在证明 $lD(R)$ 可以用循环左 R-模来计算．

引理 11.133 左 R-模 B 是内射的当且仅当对每个左理想 I，$\mathrm{Ext}_R^1(R/I,B)=\{0\}$.

证明 如果 B 是内射模，则对每个右 R-模 A，$\mathrm{Ext}_R^1(A,B)$ 为零．反之，假定对每个左理想 I，$\mathrm{Ext}_R^1(R/I,B)=\{0\}$．运用 $\mathrm{Hom}_R(\ ,B)$ 到正合列 $0\to I\to R\to R/I\to 0$ 上得

$$\mathrm{Hom}_R(R,B)\to \mathrm{Hom}_R(I,B)\to \mathrm{Ext}_R^1(R/I,B)=0.$$

的正合性．即每个 R-映射 $f: I\to B$ 可以扩张为 R-映射 $R\to B$（见命题 7.63）．但这正是白尔判别法，即定理 7.68，因此 B 是内射的． ■

下一结果说明 $lD(R)$ 可以用有限生成 R-模 M 的 $pd(M)$ 来计算；事实上，$lD(R)$ 甚至可以用循环模 M 的 $pd(M)$ 来计算．

定理 11.134（奥斯兰德） 对任意环 R，

$$lD(R)=\sup\{pd(R/I): I \text{ 是左理想}\}.$$

证明（Matlis） 如果 $\sup\{pd(R/I)\}=\infty$，证明已经完成．所以可以假定存在整数 $n\geqslant 0$ 使

得对每个左理想 I, $pd(R/I) \leqslant n$. 根据引理 11.130，对每个左 R-模 B, $\mathrm{Ext}_R^{n+1}(R/I,B)=\{0\}$. 但根据定理 11.132, $lpD(R)=liD(R)$，从而只需证明对每个 B, $id(B)\leqslant n$. 设 $\mathbf{E}^{\bullet}$ 是 B 的一个内射分解，有 $(n-1)$ 次上合冲 $\mho^{n-1}(B)$. 根据系 11.128, $\{0\}=\mathrm{Ext}_R^{n+1}(R/I,B)\cong \mathrm{Ext}_R^1(R/I,\mho^{n-1}(B))$. 现在引理 11.133 给出 $\mho^{n-1}(B)$ 是内射的，从而引理 11.130 给出所要的 $id(B)\leqslant n$. ■

这个定理解释了为什么戴得金环中的每个理想都是投射的.

正如 Ext 定义了环 R 的整体维数一样，可以用 Tor 来定义环 R 的弱维数（或 Tor-维数）.

定义 设 R 是环并设 A 是右 R-模. A 的一个**平坦分解**是指一个正合列

$$\cdots \to F_n \to \cdots \to F_1 \to F_0 \to A \to 0,$$

其中每个 F_n 都是平坦右 R-模.

如果存在有限平坦分解

$$0 \to F_n \to \cdots \to F_1 \to F_0 \to A \to 0,$$

则记 $fd(A)\leqslant n$. 如果 $n\geqslant 0$ 是使得 $fd(A)\leqslant n$ 的最小整数，则我们说 A 有**平坦维数** n；如果不存在 A 的有限平坦分解，则 $fd(A)=\infty$.

例 11.135 （ⅰ）模 A 是平坦的当且仅当 $fd(A)=0$. 我们可以认为 $fd(A)$ 测量了 A 离开平坦性的程度.

（ⅱ）因投射模是平坦的，A 的每个投射分解都是平坦分解. 由此，如果 R 是任意环，则对每个 R-模 A, $fd(A)\leqslant pd(A)$.

（ⅲ）如果 R 是戴得金环且 A 是 R-模，则根据（ⅱ），$fd(A)\leqslant pd(A)\leqslant 1$. 系 11.109 说每个无挠 R-模是平坦的（逆命题也真）. 因此 $fd(A)=1$ 当且仅当 A 不是无挠的. ■

定义 设 $\mathbf{F}_{\bullet}=\cdots \to F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{\varepsilon} A \to 0$ 是模 A 的平坦分解. 如果 $n\geqslant 0$，则 n 次轭是指

$$Y_n(A,\mathbf{F}_{\bullet})=\begin{cases}\ker\varepsilon & \text{如果 } n=0\\ \ker d_n & \text{如果 } n\geqslant 1.\end{cases}$$

术语轭（yoke）并不标准；它是希腊字 συζυγία (syzygy) 的翻译.

命题 11.136 对每个 $n\geqslant 1$，对一切右 R-模 A 和左 R-模 B，以及对 A 的每个平坦分解 $\mathbf{F}_{\bullet}$，存在同构

$$\mathrm{Tor}_{n+1}^R(A,B)\cong \mathrm{Tor}_1^R(A,Y_{n-1}(B,\mathbf{F}_{\bullet})).$$

证明 命题 11.121 证明的对偶. ■

系 11.137 对每个右 R-模 A 和左 R-模 B，对一切 $n\geqslant 0$ 以及 B 的任意平坦分解 $\mathbf{F}_{\bullet}$ 和 $\mathbf{F}'_{\bullet}$，存在同构

$$\mathrm{Tor}_1^R(A,Y_n(B,\mathbf{F}_{\bullet}))\cong \mathrm{Tor}_1^R(A,Y_n(B,\mathbf{F}'_{\bullet})).$$

证明 系 11.122 证明的对偶. ■

引理 11.138 对右 R-模 A 下列条件等价：

（ⅰ）$fd(A)\leqslant n$.

（ⅱ）对一切 $k\geqslant n+1$ 和一切左 R-模 B, $\mathrm{Tor}_k^R(A,B)=\{0\}$.

（ⅲ）对一切左 R-模 B, $\mathrm{Tor}_{n+1}^R(A,B)=\{0\}$.

（ⅳ）对 A 的每个平坦分解 $\mathbf{F}^{\bullet}$，$(n-1)$ 次轭 $Y_{n-1}(A,\mathbf{F}^{\bullet})$ 是平坦的.

（V）存在 A 的平坦分解 $\mathbf{F}^{\bullet}$ 使得 $(n-1)$ 次轭 $Y_{n-1}(A,\mathbf{F}^{\bullet})$ 是平坦的．

证明　和引理 11.123 的证明相同． ■

定义　环 R 的**右弱维数**定义为

$$rwD(R)=\sup\{fd(A):A\in\text{obj}(\mathbf{Mod}_R)\}.$$

命题 11.139　对任意环 R，$rwD(R)\leqslant n$ 当且仅当对每个左 R-模 B，$\text{Tor}_{n+1}^R(A,B)=\{0\}$．

证明　从引理 11.138 立即可得． ■

可以用明显的方式定义左 R-模的平坦维数．

定义　环 R 的**左弱维数**定义为

$$lwD(R)=\sup\{fd(B):B\in\text{obj}({}_R\mathbf{Mod})\}.$$

定理 11.140　对任意环 R，

$$rwD(R)=lwD(R).$$

证明　如果两个维数都是有限的，则左或右弱维数都是对一切右 R-模 A 和一切左 R-模 B 满足 $\text{Tor}_{n+1}^R(A,B)=\{0\}$ 的最小 $n\geqslant 0$． ■

定义　环 R 的**弱维数**是指 $rwD(R)$ 和 $lwD(R)$ 的公共值，记为 $wD(R)$．

我们早先注明存在这样的（非交换的）环，它的左整体维数和右整体维数不同．与之相比，弱维数没有左右的区别，因为张量和 Tor 同时涉及左和右两个模．

例 11.141　环 R 有 $wD(R)=0$ 当且仅当每个模都是平坦的．这些环原来是**冯・诺伊曼正则**：对每个 $a\in R$，存在 $a'\in R$ 使得 $aa'a=a$．这种环的例子是布尔环（对一切 $r\in R$ 满足 $r^2=r$ 的环R）和 $\text{End}_k(V)$，其中 V 是域 k 上的向量空间（可以是无限维的）．见 Rotman 所著的《An Introduction to Homological Algebra》，119～120 页． ■

下一命题解释为什么叫做弱维数．

命题 11.142　对任意环 R，

$$wD(R)\leqslant\min\{lD(R),rD(R)\}.$$

证明　只需证明对任意右 R-模 A，$fd(A)\leqslant pd(A)$．如果 $pd(A)=\infty$，则不需要再证明了；如果 $pd(A)\leqslant n$，存在投射分解

$$0\to P_n\to\cdots\to P_0\to A\to 0.$$

因每个投射模都是平坦的，这是一个平坦分解，表明 $fd(A)\leqslant n$．因此，$wD(R)\leqslant rD(R)$．类似的论证可证明 $wD(R)\leqslant lD(R)$． ■

系 11.143　假设对一切左 R-模 A 和 B，$\text{Ext}_R^n(A,B)=\{0\}$，则对一切右 R-模 C 和一切左R-模 D，$\text{Tor}_n^R(C,D)=\{0\}$．

证明　如果对一切 A，B，$\text{Ext}_R^n(A,B)=\{0\}$，则 $lD(R)\leqslant n-1$；如果有某个 C，D 使得 $\text{Tor}_n^R(C,D)\neq\{0\}$，则 $n\leqslant wD(DR)$．这与命题 11.142 矛盾：

$$lD(R)\leqslant n-1<n\leqslant wD(R).$$ ■

引理 11.144　左 R-模 B 是平坦的当且仅当对每个右理想 I，$\text{Tor}_1^R(R/I,B)=\{0\}$．

证明　$0\to I\xrightarrow{i}R\to R/I\to 0$ 的正合性给出

$$0=\text{Tor}_1^R(R,B)\to\text{Tor}_1^R(R/I,B)\to I\otimes_R B\xrightarrow{i\otimes 1}R\otimes_R B$$

的正合性．所以 $i\otimes 1$ 是单射当且仅当 $\text{Tor}_1^R(R/I,B)=\{0\}$．另一方面，根据系 8.108，$B$ 是平坦的

当且仅当 $i \otimes 1$ 对每个右理想 I 是单射. ■

和整体维数一样，弱维数也可以用循环模来计算.

系 11.145 对每个环 R,

$$wd(R) = \sup\{fd(R/I) : I 是 R 的右理想\}$$
$$= \sup\{fd(R/J) : J 是 R 的左理想\}.$$

证明 和定理 11.134 的证明类似，用引理 11.144 替换引理 11.133. ■

定理 11.146 设 R 是左诺特环.

（i）如果 A 是有限生成左 R-模，则

$$pd(A) = fd(A).$$

（ii）

$$wD(R) = lD(R).$$

特别地，如果 R 是交换诺特环，则

$$wD(R) = D(R).$$

证明 （i）因为每个投射分解都是一个平坦分解，所以 $fd(A) \leqslant pd(A)$ 恒成立. 关于反过来的不等式，只要证明如果 $fd(A) \leqslant n$，则 $pd(A) \leqslant n$ 就够了. 根据引理 11.37，存在 A 的投射分解，

$$\cdots \to P_n \to \cdots \to P_0 \to A \to 0,$$

其中每个 P_i 都是有限生成的. 现在这也是一个平坦分解，从而根据引理 11.138，$fd(A) \leqslant n$ 蕴涵 $Y_n = \ker(P_{n-1} \to P_{n-2})$ 是平坦的. 但根据系 8.111（因为 R 是左诺特环），每个有限生成平坦左 R-模都是投射的，从而

$$0 \to Y_{n-1} \to P_{n-1} \to \cdots \to P_0 \to A \to 0$$

是投射分解. 所以 $pd(A) \leqslant n$.

（ii）根据定理 11.134，$lD(R)$ 是循环左 R-模的投射维数的最小上界，根据系 11.145，$wd(R)$ 是循环左 R-模的平坦维数的最小上界. 但（i）给出对每个有限生成右 R-模 A，$fd(A) = pd(A)$. 这就足以证明所要的结果. ■

我们现在计算域上的多项式环的整体维数 $D(k[x_1, \cdots, x_n])$（这个结果叫做合冲上的希尔伯特定理）.

引理 11.147 如果 $0 \to A' \to A \to A'' \to 0$ 是短正合列，则

$$pd(A'') \leqslant 1 + \max\{pd(A), pd(A')\}.$$

证明 我们可以假定右端是有限的，否则就不需要证明了；设 $pd(A) \leqslant n$ 和 $pd(A') \leqslant n$. 运用 $\mathrm{Hom}(\ ,B)$（其中 B 是任意模）到短正合列得长正合列

$$\cdots \to \mathrm{Ext}^{n+1}(A', B) \to \mathrm{Ext}^{n+2}(A'', B) \to \mathrm{Ext}^{n+2}(A, B) \to \cdots.$$

根据引理11.123(ii)，两端外面的项都是$\{0\}$，从而正合性迫使对一切 B，$\mathrm{Ext}^{n+2}(A'', B) = \{0\}$. 同一引理给出 $pd(A'') \leqslant n+1$. ■

自此以后，我们将只考虑交换环. 我们希望比较 R 和 $R[x]$ 的整体维数，因此考虑由 R-模 M 形成的 $R[x]$-模 $R[x] \otimes_R M \cong M[x]$. 在第 9 章中，我们称这个模为 $M[x]$.

定义 如果 M 是交换环 R 上的 R-模，定义

$$M[x] = \sum_{i \geqslant 0} M_i,$$

其中对一切 i，$M_i \cong M$．如果定义

$$x\left(\sum_i x^i m_i\right)=\sum_i x^{i+1} m_i,$$

则 R-模 $M[x]$ 是一个 $R[x]$-模．

在引理 9.55 中，我们证明了如果 V 是交换环 R 上的自由 R-模，则 $V[x]$ 是自由 $R[x]$-模．下一结果把它从 $pd(V)=0$ 推广到更高维数．

引理 11.148 对每个 R-模 M，其中 R 是交换环，

$$pd_R(M)=pd_{R[x]}(M[x]).$$

证明 只需证明如果其中一个的维数有限且最多是 n，则另一个也是如此．

如果 $pd(M)\leqslant n$，则存在 R-投射分解

$$0\to P_n\to\cdots\to P_0\to M\to 0.$$

因 $R[x]$ 是自由 R-模，它是平坦 R-模，从而存在 $R[x]$-模的正合列

$$0\to R[x]\otimes_R P_n\to\cdots\to R[x]\otimes_R P_0\to R[x]\otimes_R M\to 0.$$

但 $R[x]\otimes_R M\cong M[x]$ 和 $R[x]\otimes_R P_n$ 是投射 $R[x]$-模（因为投射模是自由模的直和项）．所以 $pd_{R[x]}(M[x])\leqslant n$．

如果 $pd(M[x])\leqslant n$，则存在 $R[x]$-投射分解

$$0\to Q_n\to\cdots\to Q_0\to M[x]\to 0.$$

作为一个 R-模，$M[x]\cong\sum_{n\geqslant 1}M_n$，其中对一切 n，$M_n\cong M$．根据习题 11.69，$pd_R(M[x])=pd_R(M)$．每个投射 $R[x]$-模 Q_i 都是自由 $R[x]$-模 F_i 的 $R[x]$-直和项；更不必说 Q_i 是 F_i 的 R-直和项．但 $R[x]$ 是自由 R-模，从而 F_i 也是自由 R-模．所以作为 R-模，Q_i 是投射的，因此 $pd_R(M)\leqslant pd_{R[x]}(M[x])$．■

系 11.149 如果 R 是交换环且 $D(R)=\infty$，则 $D(R[x])=\infty$．

证明 如果 $D(R)=\infty$，则对每个整数 n，存在 R-模 M_n 使得 $n<pd(M_n)$．根据引理，$n<pd_{R[x]}(M_n[x])$，因此 $D(R[x])=\infty$．■

命题 11.150 对每个交换环 R，

$$D(R[x])\leqslant D(R)+1.$$

证明 回忆定理 9.56 的特征序列：如果 M 是 R-模且 $T:M\to M$ 是 R-映射，则存在 $R[x]$-模的正合列

$$0\to M[x]\to M[x]\to M^T\to 0,$$

其中 M^T 是 $R[x]$-模 M，它的标量乘法由 $ax^i m=aT^i(m)$ 给出．如果 M 已经是 $R[x]$-模而 $T:M\to M$ 是 R-映射 $m\mapsto xm$，则 $M^T=M$．根据引理 11.147，

$$\begin{aligned}pd_{R[x]}(M)&\leqslant 1+pd_{R[x]}(M[x])\\&=1+pd_R(M)\\&\leqslant 1+D(R).\end{aligned}$$

■

我们证明反过来的不等式．

定义 设 M 是 R-模，其中 R 是交换环，如果由 $m\mapsto cm$ 给出的 R-映射 $M\to M$ 是单射，则称元素 $c\in R$ 在 M 上是**正则**的（或是 M-**正则**的）．否则，称 c 为 M 上的**零因子**；即存在某个非零 $m\in M$ 使得 $cm=0$．

开始下一定理之前，我们对记号作一个解释．假设 R 是交换环，$c\in R$，$R^*=R/Rc$．如果 M 是一个 R-模，则 M/cM 是一个 (R/Rc)-模；即 M/cM 是一个 R^*-模．另一方面，每个 R^*-模 A^* 也可以看作一个 R-模．如果 $\sigma:(R/Rc)\times A^*\to A^*$ 是给定的标量乘法，又如果 $\nu:R\to R/Rc$ 是自然映射，则 $\sigma(\nu\times 1_{A^*}):R\times A^*\to A^*$ 是标量乘法．用更实在的语言来说，如果 $r^*=r+Rc$，则

$$r^*a=ra.$$

如果用这种方法把 A^* 看作一个 R-模，就把 A^* 记为 $A^\flat$. 习题 11.72 要求证明 $M^*\cong(R/cR)\otimes_R M$ 和 $A^\flat\cong\operatorname{Hom}_R(R/cR,A^*)$，从而这种构造涉及函子的伴随对．

命题 11.151（里斯引理） 设 R 是交换环，设 $c\in R$ 既不是单位也不是零因子，并设 $R^*=R/Rc$．如果 c 在一个 R-模 M 上是正则的，则存在自然同构，对每个 R^*-模 A^* 和一切 $n\geqslant 0$，

$$\operatorname{Ext}^n_{R^*}(A^*,M/cM)\cong\operatorname{Ext}^{n+1}_R(A^\flat,M),$$

其中 $A^\flat$ 是看作 R-模的 R^*-模 A^*．

证明 回忆定理 10.45，即 Ext 函子的公理刻画．给定反变函子 $G^n:{}_{R^*}\mathbf{Mod}\to\mathbf{Ab}$ 的一个序列，其中 $n\geqslant 0$，满足：

（ⅰ）对 R^*-模的每个短正合列 $0\to A^*\to B^*\to C^*\to 0$，存在具有自然连接同态的长正合列

$$\cdots\to G^n(C^*)\to G^n(B^*)\to G^n(A^*)\to G^{n+1}(C^*)\to\cdots;$$

（ⅱ）有某个 R^*-模 L^* 使得 G^0 和 $\operatorname{Hom}_{R^*}(\ ,L^*)$ 自然等价；

（ⅲ）对一切投射 R^*-模 P^* 和一切 $n\geqslant 1, G^n(P^*)=0$；

则对一切 $n\geqslant 0$，G^n 和 $\operatorname{Ext}^n_{R^*}(\ ,L^*)$ 自然等价．

定义反变函子 $G^n:{}_{R^*}\mathbf{Mod}\to\mathbf{Ab}$ 为 $G^n=\operatorname{Ext}^{n+1}_R(\ ^\flat,M)$．于是，对一切 R^*-模 A^*，

$$G^n(A^*)=\operatorname{Ext}^{n+1}_R(A^\flat,M).$$

因公理（ⅰ）对函子 Ext^n 成立，它对函子 G^n 也成立．我们证明公理（ⅱ）．定义为 $m\mapsto cm$ 的映射 $\mu_c:M\to M$ 是单射，这是因为 c 是 M-正则的，从而序列 $0\to M\xrightarrow{\mu_c}M\to M/cM\to 0$ 是正合的．考虑长正合列的一部分，其中 A^* 是 R^*-模：

$$\operatorname{Hom}_R(A^\flat,M)\to\operatorname{Hom}_R(A^\flat,M/cM)\xrightarrow{\partial}\operatorname{Ext}^1_R(A^\flat,M)\xrightarrow{(\mu_c)_*}\operatorname{Ext}^1_R(A^\flat,M).$$

我们断言∂是同构．如果 $a\in A^\flat$，则因 A^* 是 R^*-模，从而 $ca=0$（记住 $R^*=R/cR$）．因此，如果 $f\in\operatorname{Hom}_R(A^\flat,M)$，则 $cf(a)=f(ca)=f(0)=0$．因 $\mu_c:M\to M$ 是单射，对一切 $a\in A^\flat$，$f(a)=0$. 于是，$f=0$，$\ker\partial=\operatorname{Hom}_R(A^\flat,M)=\{0\}$，$\partial$是单射．根据例 10.60，映射 $(\mu_c)_*:\operatorname{Ext}^1_R(A^\flat,M)\to\operatorname{Ext}^1_R(A^\flat,M)$ 是乘 c 的映射．另一方面，例 10.70 表明如果 $\mu'_c:A^\flat\to A^\flat$ 是乘 c 的映射，则 Ext 上的诱导映射 $(\mu'_c)^*$ 也是乘 c 的映射．但因为 A^* 是 (R/cR)-模，所以 $\mu'_c=0$，从而 $(\mu'_c)^*=0$．因此，$(\mu_c)_*=(\mu'_c)^*=0$．所以 $\operatorname{im}\partial=\ker(\mu_c)_*=\operatorname{Ext}^1_R(A^\flat,M)$，从而$\partial$是满射. 由此

$$\partial:\operatorname{Hom}_R(A^\flat,M/cM)\to\operatorname{Ext}^1_R(A^\flat,M)$$

是同构，因为它是连接同态，所以是自然的．根据习题 11.70，存在自然同构

$$\operatorname{Hom}_{R^*}(A^*,M/cM)\to\operatorname{Hom}_R(A^\flat,M/cM).$$

复合

$$\operatorname{Hom}_{R^*}(A^*,M/cM)\to\operatorname{Hom}_R(A^\flat,M/cM)\to\operatorname{Ext}^1_R(A^\flat,M)=G^0(A^*)$$

是自然同构；因此它的逆定义了一个自然等价

$$G^0 \to Hom_{R^*}(\ \ ,\ M/cM)\ .$$

令 $L^* = M/cM$ 就完成了公理（ii）的验证.

剩下要验证公理（iii）：只要 P^* 是投射 R^*-模且 $n\geqslant 1$，就有 $G^n(P^*)=\{0\}$. 事实上，因 G^n 是加性函子且因每个投射模是一个自由模的直和项，我们可以假定 P^* 是自由 R^*-模，它的基比如说是 E. 如果 $Q=\sum_{e\in E} Re$ 是以 E 为基的自由 R-模，则存在 R-模的正合列

$$0 \to Q \xrightarrow{\mu_c} Q \to P^* \to 0. \tag{6}$$

因为 c 不是 R 中的零因子，所以第一个箭头是单射；最后一个箭头是满射，这是因为

$$\begin{aligned} Q/c\,Q &= \Big(\sum_{e\in E} Re\Big)\Big/\Big(\sum_{e\in E} Rce\Big) \\ &\cong \sum_{e\in E}(R/Rc)e = \sum R^* e = P^*\ . \end{aligned}$$

由（6）形成的长正合列是

$$\cdots \to \mathrm{Ext}_R^n(Q,M) \to \mathrm{Ext}_R^{n+1}(P^\flat,M) \to \mathrm{Ext}_R^{n+1}(Q,M) \to \cdots.$$

因 Q 是 R-自由的且 $n\geqslant 1$，所以外面的项都是 $\{0\}$，且正合性给出 $G^n(P^*)=\mathrm{Ext}_R^{n+1}(P^\flat,M)=\{0\}$. 所以，

$$\mathrm{Ext}_R^{n+1}(A^\flat,M) = G^n(A^*) \cong \mathrm{Ext}_{R^*}^n(A^*,M/cM). \quad ■$$

定理 11.152 对每个交换环 R，

$$D(k[x]) = D(k)+1.$$

证明 我们在命题 11.150 中已经证明 $D(k[x])\leqslant D(k)+1$，从而只需证明反过来的不等式.

在里斯引理即命题 11.151 的记号中令 $R=k[x], c=x, R^*=k$. 设 A 是有 $pd(A)=n$ 的 k-模. 根据习题 11.65，存在自由 k-模 F 使得 $\mathrm{Ext}_k^n(A,F)\neq\{0\}$；当然，乘 x 的映射是单射 $F\to F$. 和里斯引理的证明一样，存在自由 $k[x]$-模 $Q=k[x]\otimes_k F$ 使得 $Q/xQ\cong F$. 里斯引理给出

$$\mathrm{Ext}_{k[x]}^{n+1}(A,Q) \cong \mathrm{Ext}_k^n(A,Q/xQ) \cong \mathrm{Ext}_k^n(A,F) \neq \{0\}$$

（把 A 看作经由 $k[x]\to k$ 的 $k[x]$-模）. 所以 $pd_{k[x]}(A)\geqslant n+1$，因此 $D(k[x])\geqslant n+1=D(k)+1$.

■

系 11.153（合冲上的希尔伯特定理） 如果 k 是域，则

$$D(k[x_1,\cdots,x_n]) = n.$$

证明 因对每个域 k, $D(k)=0$ 和 $D(k[x])=1$，由定理 11.152 对 $n\geqslant 0$ 用归纳法可得结果.

■

合冲上的希尔伯特定理蕴涵如果 $R=k[x_1,\cdots,x_n]$，其中 k 是域，则每个有限生成 R-模 M 有分解

$$0 \to P_n \to P_{n-1} \to \cdots \to P_0 \to M \to 0,$$

其中对一切 $i<n$，P_i 是自由的且 P_n 是投射的. 我们说在任意交换环 R 上的一个 R-模 M（必须是有限生成的）有 FFR（有限自由分解），如果它有这样的一个分解，其中每个 P_i（包括最后一个 P_n）都是有限生成自由模. 合冲上的希尔伯特定理可以改进为如下的定理：如果 k 是域，则每个有限生成 $k[x_1,\cdots,x_n]$-模都有 FFR（见 Kaplansky 所著的《Commutative Rings》，134 页）.（当然，这个结果也可以从更难的奎伦-苏斯林定理得到，该定理说每个投射 $k[x_1,\cdots,x_n]$-模都是自由

的，其中 k 是域．）

习题

11.62 （ⅰ）如果 $A \to B \xrightarrow{f} C \to D$ 是正合列，又如果 X 是任意模，证明存在正合列

$$A \to B \oplus X \xrightarrow{f \oplus 1_X} C \oplus X \to D.$$

（ⅱ）设

$$\mathbf{P}_\bullet = \cdots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} A \to 0$$

和

$$\mathbf{P}'_\bullet = \cdots \to P'_2 \xrightarrow{d'_2} P'_1 \xrightarrow{d'_1} P'_0 \xrightarrow{\varepsilon'} A \to 0$$

都是左 R-模 A 的投射分解．证明：对一切 $n \geqslant 0$，存在投射模 Q_n 和 Q'_n 使得

$$\Omega_n(A, \mathbf{P}_\bullet) \oplus Q_n \cong \Omega_n(A, \mathbf{P}'_\bullet) \oplus Q'_n.$$

提示：对 $n \geqslant 0$ 用归纳法，并用 Schanuel 引理，即命题 7.60.

11.63 设

$$0 \to B \to E^0 \to E^1 \to E^2 \to \cdots$$

和

$$0 \to B \to E'^0 \to E'^1 \to E'^2 \to \cdots$$

都是左 R-模 B 的内射分解．证明：对一切 $n \geqslant 0$，存在内射模 I_n 和 I'_n 使得

$$\mho^n(B, \mathbf{E}^\bullet) \oplus I_n \cong \mho^n(B, \mathbf{E}'^\bullet) \oplus I'_n.$$

提示：这个证明是习题 11.62 的对偶．

11.64 证明存在平坦分解

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

和

$$0 \to K \to F \to \mathbb{Q}/\mathbb{Z} \to 0,$$

其中 F 是自由阿贝尔群，但 $\mathbb{Z} \oplus F \ncong \mathbb{Q} \oplus K$.

11.65 如果 A 是有 $pd(A) = n$ 的 R-模，证明存在自由 R-模 F 使得 $\mathrm{Ext}_R^n(A, F) \neq \{0\}$.

提示：每个模都是自由模的商．

11.66 如果 G 是阶不等于 1 的有限循环群，证明

$$lD(\mathbb{Z}G) = \infty = rD(\mathbb{Z}G).$$

提示：用定理 10.107.

11.67 （奥斯兰德）如果 R 既是左诺特环又是右诺特环，证明

$$lD(R) = rD(R).$$

提示：用弱维数．

11.68 证明冯·诺伊曼正则诺特环是半单环．

提示：见例 11.141.

11.69 如果 $\{M_\alpha : \alpha \in A\}$ 是左 R-模的族，证明

$$pd\Big(\sum_{\alpha \in A} M_\alpha\Big) = \sup_{\alpha \in A}\{pd(M_\alpha)\}.$$

11.70 如果 $\varphi: R \to R^*$ 是环同态且 A^*, B^* 都是 R^*-模，证明存在自然同构

$$\mathrm{Hom}_{R^*}(A^*, B^*) \to \mathrm{Hom}_R(A^\flat, B^\flat),$$

其中 $A^\flat$ 是看作 R-模的 A^*.

11.71 (i) 如果 $0 \to A' \to A \to A'' \to 0$ 是正合列，证明

$$pd(A) \leqslant \max\{pd(A'), pd(A'')\}.$$

(ii) 如果 (i) 中的序列不分裂，又如果 $pd(A') = pd(A'') + 1$，证明

$$pd(A) = \max\{pd(A'), pd(A'')\}.$$

11.72 设 k 是交换环，$c \in k$，并设 $k^* = k/ck$.

(i) 如果 M 是 k-模，定义 $M^* = M/cM$. 证明 $M^* \cong (k/ck) \otimes_k M$.

(ii) 如果 A^* 是 k^*-模 A^*，定义 $A^\flat$ 为看作 K-模的 A^*. 证明 $A^\flat \cong \mathrm{Hom}_k(k/ck, A^*)$. 由此推出 $M \mapsto M^*$ 和 $A^* \mapsto A^\flat$ 形成函子的伴随对.

11.73 设 $\varphi: k \to k^*$ 是环同态.

(i) 证明 k^* 是 (k^*, k)-双模.

(ii) 证明每个 k^*-模 A^* 都可看作一个 k-模，记为 $A^\flat$，且 $A^* \mapsto A^\flat$ 给出正合函子 $U: {}_{k^*}\mathbf{Mod} \to {}_k\mathbf{Mod}$.

(iii) 证明：如果 $F = \mathrm{Hom}_k(k^*, \ ): {}_k\mathbf{Mod} \to {}_{k^*}\mathbf{Mod}$，则 (U, F) 和 (F, U) 是函子的伴随对.（这种函子叫做**环的替换**函子.）由此推出 U 和 F 保持一切正向极限和一切反向极限.

11.74 设 R 是有 FFR 的交换环. 证明每个有限生成投射 R-模 P 都有自由补；即存在有限生成自由 R-模 F 使得 $P \oplus F$ 是自由 R-模.

11.4 正则局部环

我们现在要关注（交换）诺特局部环，主要结果是这种环有有限整体维数当且仅当它是*正则局部环*（正则局部环是在代数几何中十分自然地形成的），而且它们都是 UFD. 我们从一个局部化结果开始.

命题 11.154 *设 R 是交换诺特环.*

(i) 如果 A 是有限生成 R-模，则

$$pd(A) = \sup_{\mathfrak{m}} pd(A_{\mathfrak{m}}),$$

其中 $\mathfrak{m}$ 遍历 R 的一切极大理想.

(ii)

$$D(R) = \sup_{\mathfrak{m}} D(R_{\mathfrak{m}}),$$

其中 $\mathfrak{m}$ 遍历 R 的一切极大理想.

证明 (i) 我们先对每个极大理想 $\mathfrak{m}$ 证明 $pd(A) \geqslant pd(A_{\mathfrak{m}})$. 如果 $pd(A) = \infty$，则没有什么可证明的，因此可以假定 $pd(A) = n < \infty$. 于是存在投射分解

$$0 \to P_n \to P_{n-1} \to \cdots \to P_0 \to A \to 0.$$

因 $R_{\mathfrak{m}}$ 是平坦 R-模，根据定理 11.28，

$$0 \to R_{\mathfrak{m}} \otimes P_n \to R_{\mathfrak{m}} \otimes P_{n-1} \to \cdots \to R_{\mathfrak{m}} \otimes P_0 \to A_{\mathfrak{m}} \to 0$$

是 $A_{\mathfrak{m}}$ 的投射分解，从而 $pd(A_{\mathfrak{m}}) \leqslant n$.（这个推断不需要假设 R 是诺特环或 A 是有限生成的.）

关于反过来的不等式，只需假定 $\sup_{\mathfrak{m}} pd(A_{\mathfrak{m}}) = n < \infty$ 就够了. 因 R 是诺特环，定理11.146 (i) 说 $pd(A) = fd(A)$. 现在根据引理 11.138，$pd(A_{\mathfrak{m}}) \leqslant n$ 当且仅当对一切 $R_{\mathfrak{m}}$-模 $B_{\mathfrak{m}}$，$\mathrm{Tor}_{n+1}^{R_{\mathfrak{m}}}(A_{\mathfrak{m}}, B_{\mathfrak{m}})$

$=\{0\}$. 然而命题 11.35 给出同构 $\mathrm{Tor}_{n+1}^{R_\mathfrak{m}}(A_\mathfrak{m},B_\mathfrak{m})\cong(\mathrm{Tor}_{n+1}^R(A,B))_\mathfrak{m}$. 所以根据命题 11.31（i），$\mathrm{Tor}_{n+1}^R(A,B)=\{0\}$. 由此可知 $n\geqslant pd(A)$.

（ii）从（i）立得，因为根据定理 11.134，$D(R)=\sup_A\{pd(A)\}$，其中 A 遍历一切有限生成（甚至是循环）R-模. ■

我们现在设置本节以后要用到的记号.

记号 *我们记交换诺特局部环为 R，$(R,\mathfrak{m})$ 或 $(R,\mathfrak{m},k)$，其中 $\mathfrak{m}$ 是它唯一的极大理想而 k 是它的***剩余域** *$k=R/\mathfrak{m}$.*

定理 11.134 使我们可以计算整体维数，并把它作为循环模的投射维数的最小上界. 当 R 是局部环时，有一个惊人的改进：整体维数由一个循环模的投射维数确定：它就是剩余域 k.

引理 11.155 *设 $(R,\mathfrak{m})$ 是有剩余域 k 的局部环. 如果 A 是有限生成 R-模，则*

$$pd(A)\leqslant n \text{ 当且仅当 } \mathrm{Tor}_{n+1}^R(A,k)=\{0\}.$$

证明 假定 $pd(A)\leqslant n$. 根据例 11.135（ii）有 $fd(A)\leqslant pd(A)$，从而对每个 R-模 B，$\mathrm{Tor}_{n+1}^R(A,B)=\{0\}$. 特别地，$\mathrm{Tor}_{n+1}^R(A,k)=\{0\}$.

我们对 $n\geqslant 0$ 用归纳法证明逆命题. 关于基础步 $n=0$，需要证明 $\mathrm{Tor}_1^R(A,k)=\{0\}$ 蕴涵 $pd(A)=0$；即 A 是投射的（因为 R 是局部环，因此是自由的）. 设 $\{a_1,\cdots,a_r\}$ 是 A 的生成元的极小集（即没有真子集能够生成 A），设 F 是以 $\{e_1,\cdots,e_r\}$ 为基的自由 R-模，并设 $\varphi:F\to A$ 是满足 $\varphi(e_i)=a_i$ 的 R-映射. 存在正合列

$$0\to N\xrightarrow{i}F\xrightarrow{\varphi}A\to 0,$$

其中 $N=\ker\varphi$ 且 i 是包含映射；和命题 11.23 的证明一样，

$$N\subseteq\mathfrak{m}F.$$

因 $\mathrm{Tor}_1^R(A,k)=\{0\}$，序列

$$0\to N\otimes_R k\xrightarrow{i\otimes 1}F\otimes_R k\xrightarrow{\varphi\otimes 1}A\otimes_R k\to 0$$

是正合的. 用 N 对 $0\to\mathfrak{m}\to R\to k\to 0$ 作张量积；右正合性给出自然同构

$$\tau_N:N\otimes_R k\to N/\mathfrak{m}N;$$

如果 $n\in N$ 和 $b\in k$，则 $\tau_N:n\otimes b\mapsto n+\mathfrak{m}N$. 存在交换图

$$\begin{array}{ccccc} 0 & \longrightarrow & N\otimes_R k & \xrightarrow{i\otimes 1} & F\otimes_R k \\ & & \downarrow{\scriptstyle \tau_N} & & \downarrow{\scriptstyle \tau_F} \\ & & N/\mathfrak{m}N & \xrightarrow[\bar{i}]{} & F/\mathfrak{m}F \end{array}$$

其中 $\bar{i}:n+\mathfrak{m}N\mapsto n+\mathfrak{m}F$. 因 $i\otimes 1$ 是单射，从而 $\bar{i}$ 也是单射. 但 $N\subseteq\mathfrak{m}F$ 说明映射 $\bar{i}$ 是零映射. 所以 $N/\mathfrak{m}N=\{0\}$，从而 $N=\mathfrak{m}N$. 根据 Nakayama 引理，即系 8.32，$N=\{0\}$，因此 $\varphi:F\to A$ 是同构；即 A 是自由的.

关于归纳步，我们需要证明如果 $\mathrm{Tor}_{n+1}^R(A,k)=\{0\}$，则 $pd(A)\leqslant n+1$. 取 A 的投射分解 $\mathbf{P}_\bullet$，并设 $\Omega_n(A,\mathbf{P}_\bullet)$ 是它的 n 次合冲. 因 $\mathbf{P}_\bullet$ 必定也是 A 的平坦分解，有 $Y_n(A,\mathbf{P}_\bullet)=\Omega_n(A,\mathbf{P}_\bullet)$. 根据命题 11.136，$\mathrm{Tor}_{n+2}^R(A,k)\cong\mathrm{Tor}_1^R(Y_n(A,\mathbf{P}_\bullet),k)$. 基础步证明 $Y_n(A,\mathbf{P}_\bullet)=\Omega_n(A,\mathbf{P}_\bullet)$ 是自由的，由此根据引理 11.123 得 $pd(A)\leqslant n+1$. ■

系 11.156 *设 $(R,\mathfrak{m})$ 是有剩余域 k 的局部环. 如果 A 是有限生成 R-模，则*

$$pd(A) = \sup\{i : \mathrm{Tor}_i^R(A,k) \neq \{0\}\}.$$

证明 设 $n = \sup\{i : \mathrm{Tor}_i^R(A,k) \neq \{0\}\}$，则 $pd(A) \leqslant n-1$，但 $pd(A) \not< n$；即 $pd(A) = n$. ■

定理 11.157 设 R 是有剩余域 k 的局部环.

(i)

$$D(R) \leqslant n \quad 当且仅当 \quad \mathrm{Tor}_{n+1}^R(k,k) = \{0\}.$$

(ii)

$$D(R) = pd(k).$$

证明 (i) 如果 $D(R) \leqslant n$，则用引理 11.155 立刻得到 $\mathrm{Tor}_{n+1}^R(k,k) = \{0\}$. 反之，如果 $\mathrm{Tor}_{n+1}^R(k,k) = \{0\}$，同一引理给出 $pd(k) \leqslant n$. 根据引理 11.138，对每个 R-模 A 有 $\mathrm{Tor}_{n+1}^R(A,k) = \{0\}$. 特别地，如果 A 是有限生成的，则引理 11.155 给出 $pd(A) \leqslant n$. 最后，定理 11.134 证明 $D(R) = \sup_A\{pd(A)\}$，其中 A 遍历一切有限生成（甚至是循环的）R-模. 所以 $D(R) \leqslant n$.

(ii) 从 (i) 立即可得. ■

定义 交换环 R 中长度为 n 的一个**素链**是指素理想的一个严格降链

$$\mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_n.$$

一个素理想 $\mathfrak{p}$ 的**高度** $\mathrm{ht}(\mathfrak{p})$ 是指有 $\mathfrak{p} = \mathfrak{p}_0$ 的最长素链的长度. 于是，$\mathrm{ht}(\mathfrak{p}) \leqslant \infty$.

例 11.158 (i) 如果 $\mathfrak{p}$ 是素理想，则 $\mathrm{ht}(\mathfrak{p}) = 0$ 当且仅当 $\mathfrak{p}$ 是极小素理想. 如果 R 是整环，则 $\mathrm{ht}(\mathfrak{p}) = 0$ 当且仅当 $\mathfrak{p} = \{0\}$.

(ii) 如果 R 是戴得金环且 $\mathfrak{p}$ 是 R 中的非零素理想，则 $\mathrm{ht}(\mathfrak{p}) = 1$.

(iii) 设 k 是域并设 $R = k[X]$ 是有无限个变量 $X = \{x_1, x_2, \cdots\}$ 的多项式环. 如果 $\mathfrak{p}_i = (x_i, x_{i+1}, \cdots)$，则 $\mathfrak{p}_i$ 是素理想（$R/\mathfrak{p}_i \cong k[x_1, \cdots, x_{i-1}]$ 是整环）且对每个 $n \geqslant 1$，

$$\mathfrak{p}_1 \supsetneq \mathfrak{p}_2 \supsetneq \cdots \supsetneq \mathfrak{p}_{n+1}$$

是长度为 n 的素链. 由此 $\mathrm{ht}(\mathfrak{p}_1) = \infty$. ■

定义 如果 R 是交换环，则它的**克鲁尔维数**是

$$\dim(R) = \sup\{\mathrm{ht}(\mathfrak{p}) : \mathfrak{p} \in \mathrm{Spec}(R)\};$$

即 $\dim(R)$ 是 R 中最长素链的长度.

如果 R 是戴得金环，则 $\dim(R) = 1$，这是因为每个非零素理想都是极大理想. 如果 R 是整环，则 $\dim(R) = 0$ 当且仅当 R 是域. 下一命题刻画了克鲁尔维数为 0 的诺特环.

命题 11.159 如果 R 是诺特环，则 $\dim(R) = 0$ 当且仅当每个有限生成 R-模 M 都有合成列.

证明 假定 R 是克鲁尔维数为 0 的诺特环. 因 R 是诺特环，系 6.120(iii) 说只有有限个极小素理想. 因 $\dim(R) = 0$，每个素理想都是极小素理想（也是极大素理想）. 由此可知 R 只有有限个素理想，比如 $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$. 现在根据习题 11.39，$\mathrm{nil}(R) = \bigcap_{i=1}^{n} \mathfrak{p}_i$ 是幂零的；比如 $(\mathrm{nil}(R))^m = \{0\}$. 定义

$$N = \mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n = \mathrm{nil}(R),$$

从而

$$N^m = (\mathfrak{p}_1 \cdots \mathfrak{p}_n)^m = \{0\}.$$

设 M 是有限生成 R-模，考虑链

$$M \supseteq \mathfrak{p}_1 M \supseteq \mathfrak{p}_1 \mathfrak{p}_2 M \supseteq \cdots \supseteq NM.$$

因子模 $\mathfrak{p}_1\cdots\mathfrak{p}_{i-1}M/\mathfrak{p}_1\cdots\mathfrak{p}_iM$ 是 $(R/\mathfrak{p}_i)$-模；即它是域 $R/\mathfrak{p}_i$ 上的向量空间（因为 $\mathfrak{p}_i$ 是极大理想）．因 M 是有限生成的，因子模的维数有限，从而链可以加细使得一切因子模都是单的．最后，对链

$$N^jM \supseteq \mathfrak{p}_1 N^jM \supseteq \mathfrak{p}_1\mathfrak{p}_2 N^jM \supseteq \cdots \supseteq N^{j+1}M$$

重复这个论证．因 $N^m=\{0\}$，所以我们已经构造了 M 的一个合成列．

反之，如果每个有限生成 R-模都有合成列，则循环 R-模 R 有合成列；比如长度为 ℓ. 由此，任一理想的升链的长度最多是 ℓ，因此 R 是诺特的．为证明 $\dim(R)=0$，我们需要证明 R 不包含任何素理想 $\mathfrak{p}\supsetneq\mathfrak{q}$. 可以转到商环 $R/\mathfrak{q}$ 并重述假设：R 是有一个非零素理想和合成列 $R\supseteq I_1\supseteq\cdots\supseteq I_d\neq\{0\}$ 的整环．最后一个理想 I_d 是极小理想；选取一个非零元素 $x\in I_d$．当然，$xI_d\subseteq I_d$；因 R 是整环，$xI_d\neq\{0\}$，从而 I_d 的极小性给出 $xI_d=I_d$．因此存在 $y\in I_d$ 使得 $xy=x$；即 $1=y\in I_d$，从而 $I_d=R$．由此可知 R 是域，与它有非零素理想矛盾． ■

我们将证明克鲁尔的一个定理，即**主理想定理**，它蕴涵诺特环中的每个素理想都有有限高度．我们的证明是 Kaplansky 对里斯证明的修改．下面从一个技术性引理开始．

引理 11.160 *设 a 和 b 是整环 R 中的非零元素．如果存在 $c\in R$ 满足 $ca^2\in(b)$ 蕴涵 $ca\in(b)$，则列 $(a,b)\supseteq(a)\supseteq(a^2)$ 和 $(a^2,b)\supseteq(a^2,ab)\supseteq(a^2)$ 有同构的因子模．*[⊖]

证明 因为乘 a 的映射把 (a,b) 送到 (a^2,ab) 上和把 (a) 送到 (a^2) 上，所以 $(a,b)/(a)\cong(a^2,ab)/(a^2)$．

模 $(a)/(a^2)$ 是有零化子 (a) 的循环模；即 $(a)/(a^2)\cong R/(a)$．因为生成元 a^2 在 (a^2,ab) 中，所以模 $(a^2,b)/(a^2,ab)$ 也是循环模．现在 $A=\operatorname{ann}((a^2,b)/(a^2,ab))$ 包含 (a)，从而只需证明 $A=(a)$；即如果 $cb=ua^2+vab$，则 $c\in(a)$．这个等式给出 $ua^2\in(b)$，从而假设给出某个 $r\in R$ 使得 $ua=rb$．代入得 $cb=rab+vab$，消去 b 得 $c=ra+va\in(a)$．所以 $(a)/(a^2)\cong(a^2,b)/(a^2,ab)$． ■

回忆素理想 $\mathfrak{p}$ 在理想 I 上极小，如果 $I\subseteq\mathfrak{p}$ 且没有素理想 $\mathfrak{q}$ 满足 $I\subseteq\mathfrak{q}\subsetneq\mathfrak{p}$.

定理 11.161（主理想定理） *设 (a) 是诺特环 R 中的真理想，并设 $\mathfrak{p}$ 是在 (a) 上极小的素理想，则 $\operatorname{ht}(\mathfrak{p})\leqslant 1$．*

证明 如果相反，$\operatorname{ht}(\mathfrak{p})\geqslant 2$，则存在素链

$$\mathfrak{p}\supsetneq\mathfrak{p}_1\supsetneq\mathfrak{p}_2.$$

我们用两种方法把问题规范化．首先把 R 换成 $R/\mathfrak{p}_2$；其次在 $\mathfrak{p}/\mathfrak{p}_2$ 上局部化．现在根据此修改假设：R 是局部整环，它的极大理想 $\mathfrak{m}$ 在一个真主理想 (x) 上极小，且存在素理想 $\mathfrak{q}$ 使得

$$\mathfrak{m}\supsetneq\mathfrak{q}\supsetneq(0).$$

选取非零元素 $b\in\mathfrak{q}$，定义

$$I_i=((b):x^i)=\{c\in R: cx^i\in(b)\}.$$

存在升链 $I_1\subseteq I_2\subseteq\cdots$，因为 R 是诺特环，它必有终止：比如 $I_n=I_{n+1}=\cdots$．由此，如果 $c\in I_{2n}$，则 $c\in I_n$；即如果 $cx^{2n}\in(b)$，则 $cx^n\in(b)$．如果令 $a=x^n$，则 $ca^2\in(b)$ 蕴涵 $ca\in(b)$．

如果 $R^*=R/(a^2)$，则因 R^* 恰有一个素理想，所以 $\dim(R^*)=0$．根据命题 11.159，R^*-模 $(a,b)/(a^2)$（和每个有限生成 R^*-模一样）有有限长度 ℓ（它的合成列的长度）．但引理 11.160 蕴涵 (a,b) 和它的子模 (a^2,b) 有相同的长度 ℓ. 若尔当-赫尔德定理说只有 $(a^2,b)=(a,b)$ 时才有可能，这就迫使 $a\in(a^2,b)$：存在 $s,t\in R$ 使得 $a=sa^2+tb$．因 $sa\in\mathfrak{m}$，元素 $1-sa$ 是单位（因为 $(R,$

⊖ 我们关于理想的记号不是一致的．由一个元素 $a\in R$ 生成的主理想有时记为 (a)，有时记为 Ra．

$\mathfrak{m}$) 是局部环). 因此, $-a(1-sa)=tb\in(b)$ 给出 $a\in(b)\subseteq\mathfrak{q}$. 但 $a=x^n$ 给出 $x\in\mathfrak{q}$, 与 $\mathfrak{m}$ 是在 (x) 上极小的素理想矛盾. ■

我们现在把主理想定理推广到有限生成理想上.

定理 11.162 (广义主理想定理) *设 $I=(a_1,\cdots,a_n)$ 是诺特环 R 中的真理想, 并设 $\mathfrak{p}$ 是在 I 上极小的素理想, 则 $\mathrm{ht}(\mathfrak{p})\leqslant n$.*

证明 在 $\mathfrak{p}$ 上局部化命题的假设仍然成立, 因此可以假定 R 是以 $\mathfrak{p}$ 作为它的极大理想的局部环.

对 $n\geqslant 1$ 用归纳法证明, 基础步是主理想定理. 设 $I=(a_1,\cdots,a_{n+1})$, 用导致矛盾的方法, 假定 $\mathrm{ht}(\mathfrak{p})>n+1$: 存在素链

$$\mathfrak{p}=\mathfrak{p}_0\supsetneqq\mathfrak{p}_1\supsetneqq\cdots\supsetneqq\mathfrak{p}_{n+1}.$$

可以假定没有素理想严格地在 $\mathfrak{p}$ 和 $\mathfrak{p}_1$ 之间, 这是因为模 $\mathfrak{p}/\mathfrak{p}_1$ 有 ACC. 现在 $I\nsubseteq\mathfrak{p}_1$, 这是因为 $\mathfrak{p}$ 是 I 上的极小素理想. 如有必要对 I 的生成元重新标号, 有 $a_1\notin\mathfrak{p}_1$. 因此 $(a_1,\mathfrak{p}_1)\supsetneqq\mathfrak{p}_1$. 我们断言 $\mathfrak{p}$ 是包含 $(a_1,\mathfrak{p}_1)$ 的唯一素理想; 不能有素理想 $\mathfrak{p}'$ 使得 $(a_1,\mathfrak{p}_1)\subseteq\mathfrak{p}'\subseteq\mathfrak{p}$ (第二个包含关系成立是因为 $\mathfrak{p}$ 是 R 中唯一的极大理想), 这是因为没有素理想严格地介于 $\mathfrak{p}$ 和 $\mathfrak{p}_1$ 之间. 所以在环 $R/(a_1,\mathfrak{p}_1)$ 中, $\mathfrak{p}$ 的象是唯一的非零素理想. 如此, 它必定是诣零根, 且因此根据习题 11.39, 它是幂零的. 存在整数 m 使得 $\mathfrak{p}^m\subseteq(a_1,\mathfrak{p}_1)$, 因此有等式

$$a_i^m=r_ia_1+b_i,r_i\in R,b_i\in\mathfrak{p}_1,i\geqslant 2. \tag{7}$$

定义 $J=\{b_2,\cdots,b_{n+1}\}$. 现在 $J\subseteq\mathfrak{p}_1$, 而 $\mathrm{ht}(\mathfrak{p}_1)>n$. 根据归纳假设, $\mathfrak{p}_1$ 不可能是在 J 上极小的素理想, 因此存在素理想 $\mathfrak{q}$ 在 J 上极小:

$$J\subseteq\mathfrak{q}\subsetneqq\mathfrak{p}_1.$$

现在对一切 i, 根据 (7) 式, $a_i^m\in(a_1,\mathfrak{q})$. 于是包含 $(a_1,\mathfrak{q})$ 的任一素理想 $\mathfrak{p}'$ 必包含一切 a_i^m, 因此包含一切 a_i, 且因此包含 I. 由于 $\mathfrak{p}$ 是唯一的极大理想, 因此 $I\subseteq\mathfrak{p}'\subseteq\mathfrak{p}$. 但 $\mathfrak{p}$ 是在 I 上极小的素理想, 从而 $\mathfrak{p}'=\mathfrak{p}$. 所以 $\mathfrak{p}$ 是包含 $(a_1,\mathfrak{q})$ 的唯一素理想. 如果 $R^*=R/\mathfrak{q}$, 则 $\mathfrak{p}^*=\mathfrak{p}/\mathfrak{q}$ 是在主理想 $(a_1+\mathfrak{q})$ 上极小的素理想. 另一方面, 因为 $\mathfrak{p}^*\supsetneqq\mathfrak{p}_1^*\supsetneqq\{0\}$ 是素链, 其中 $\mathfrak{p}_1^*=\mathfrak{p}_1/\mathfrak{q}$, 从而 $\mathrm{ht}(\mathfrak{p}^*)\geqslant 2$. 这与主理想定理矛盾, 证明完成. ■

系 11.163 *如果 R 是诺特环, 则每个素理想的高度有限, 且因此 $\mathrm{Spec}(R)$ 有 DCC.*

证明 因为 R 是诺特环, 每个素理想 $\mathfrak{p}$ 都是有限生成的; 比如 $\mathfrak{p}=(a_1,\cdots,a_n)$. 但 $\mathfrak{p}$ 是在它自身上极小的素理想, 因此定理 11.162 给出 $\mathrm{ht}(\mathfrak{p})\leqslant n$. ■

一个诺特环可能有无限克鲁尔维数, 因为素链的长度可能没有一致上界. 我们将看到这种情况对局部环是不可能发生的.

广义主理想定理限制了在一个理想上极小的素理想的高度; 下一结果限制了仅仅包含一个理想的素理想的高度.

系 11.164 *设 R 是诺特环, 设 $I=(a_1,\cdots,a_n)$ 是 R 中的理想, 并设 $\mathfrak{p}$ 是 R 中包含 I 的素理想. 如果 $\mathrm{ht}(\mathfrak{p}/I)$ 表示 $\mathfrak{p}/I$ 在 R/I 中的高度, 则*

$$\mathrm{ht}(\mathfrak{p})\leqslant n+\mathrm{ht}(\mathfrak{p}/I).$$

证明 对 $h=\mathrm{ht}(\mathfrak{p}/I)\geqslant 0$ 用归纳法证明. 如果 $h=0$, 则习题 11.76 说 $\mathfrak{p}$ 在 I 上是极小的, 从而基础步是广义主理想定理. 关于归纳步 $h>0$, $\mathfrak{p}$ 在 I 上不是极小的. 根据系 6.120 (ⅲ), R/I 中只有有限个极小素理想, 从而习题 11.76 说只有有限个素理想在 I 上极小; 比如 $\mathfrak{q}_1,\cdots,\mathfrak{q}_s$. 因 $\mathfrak{p}$ 在 I 上不是极小的, 对任意 i, $\mathfrak{p}\nsubseteq\mathfrak{q}_i$; 因此命题 6.14 说 $\mathfrak{p}\nsubseteq\mathfrak{q}_1\cup\cdots\cup\mathfrak{q}_s$, 从而存在 $y\in\mathfrak{p}$ 满足对任意

i 有 $y \notin \mathfrak{q}_i$. 定义 $J = (I, y)$.

我们现在证明在 R/J 中, $\text{ht}(\mathfrak{p}/J) \leqslant h-1$. 设

$$\mathfrak{p}/J \supsetneq \mathfrak{p}_1/J \supsetneq \cdots \supsetneq \mathfrak{p}_r/J$$

是 R/J 中的素链. 因 $I \subsetneq J$, 存在满射环映射 $R/I \to R/J$. 把这个素链提升为 R/I 中的素链:

$$\mathfrak{p}/I \supsetneq \mathfrak{p}_1/I \supsetneq \cdots \supsetneq \mathfrak{p}_r/I.$$

现在 $\mathfrak{p}_r \supseteq J \supsetneq I$, $J = (I, y)$ 不包含任一 $\mathfrak{q}_i$. 但根据习题 11.76, 理想 $\mathfrak{q}_i/I$ 是 R/I 中的极小素理想, 从而 $\mathfrak{p}_r$ 不是 R 中的极小素理想. 所以存在以 $\mathfrak{p}$ 起首、长度为 $r+1$ 的素链. 由此可知 $r+1 \leqslant h$, 从而 $\text{ht}(\mathfrak{p}/J) \leqslant h-1$.

因 $J = (I, y) = (a_1, \cdots, a_n, y)$ 是由 $n+1$ 个元素生成的, 归纳假设给出

$$\begin{aligned}\text{ht}(\mathfrak{p}) &\leqslant n+1+\text{ht}(\mathfrak{p}/J)\\ &= (n+1)+(h-1) = n+h = n+\text{ht}(\mathfrak{p}/I).\end{aligned}$$ ■

在下一命题中, 当我们说到一个理想 I 的生成集 X 为极小的时候, 是指没有 X 的真子集能够生成 I.

如果 $(R, \mathfrak{m}, k)$ 是局部环, 则 $\mathfrak{m}/\mathfrak{m}^2$ 是 $(R/\mathfrak{m})$-模; 即它是 k 上的向量空间.

命题 11.165 设 $(R, \mathfrak{m}, k)$ 是诺特局部环.

(i) 元素 $x_1, \cdots, x_d$ 形成关于 $\mathfrak{m}$ 的极小生成集当且仅当陪集 $x_i^* = x_i + \mathfrak{m}^2$ 形成 $\mathfrak{m}/\mathfrak{m}^2$ 的基.

(ii) $\mathfrak{m}$ 的任意两个极小生成集有相同的元素个数.

证明 (i) 如果 $x_1, \cdots, x_d$ 是关于 $\mathfrak{m}$ 的极小生成集, 则 $X^* = x_1^*, \cdots, x_d^*$ 张成向量空间 $\mathfrak{m}/\mathfrak{m}^2$. 如果 X^* 是线性相关的, 则有某个 $x_i^* = \sum_{j \neq i} r'_j x_j^*$, 其中 $r'_j \in k$. 把这个等式提升到 $\mathfrak{m}$, 有 $x_i \in \sum_{j \neq i} r_j x_j + \mathfrak{m}^2$. 于是, 如果 $B = \langle x_j : j \neq i \rangle$, 则 $B + \mathfrak{m}^2 = \mathfrak{m}$. 因此,

$$\mathfrak{m}(\mathfrak{m}/B) = (B + \mathfrak{m}^2)/B = \mathfrak{m}/B.$$

根据 Nakayama 引理, $\mathfrak{m}/B = \{0\}$, 从而 $\mathfrak{m} = B$. 这与 $x_1, \cdots, x_d$ 是极小生成集矛盾. 所以 X^* 是线性无关的, 因此它是 $\mathfrak{m}/\mathfrak{m}^2$ 的基.

反之, 假定 $x_1^*, \cdots, x_d^*$ 是 $\mathfrak{m}/\mathfrak{m}^2$ 的基, 其中 $x_i^* = x_i + \mathfrak{m}^2$. 如果定义 $A = \langle x_1, \cdots, x_d \rangle$, 则 $A \subseteq \mathfrak{m}$. 如果 $y \in \mathfrak{m}$, 则 $y^* = \sum r'_i x_i^*$, 其中 $r'_i \in k$, 从而 $y \in A + \mathfrak{m}^2$. 因此 $\mathfrak{m} = A + \mathfrak{m}^2$, 且和上段一样, Nakayama 引理给出 $\mathfrak{m} = A$; 即 $x_1, \cdots, x_d$ 生成 $\mathfrak{m}$. 如果 $x_1, \cdots, x_d$ 的一个真子集生成 $\mathfrak{m}$, 则向量空间 $\mathfrak{m}/\mathfrak{m}^2$ 可以由少于 d 个元素生成, 与 $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = d$ 矛盾.

(ii) 任一极小生成集中元素的个数是 $\dim_k(\mathfrak{m}/\mathfrak{m}^2)$. ■

定义 如果 $(R, \mathfrak{m}, k)$ 是诺特局部环, 则 $\mathfrak{m}/\mathfrak{m}^2$ 是 k 上有限维向量空间. 记

$$\mu(\mathfrak{m}) = \dim_k(\mathfrak{m}/\mathfrak{m}^2).$$

命题 11.165 证明 $\mathfrak{m}$ 的一切极小生成集有相同的元素个数, 就是 $\mu(\mathfrak{m})$.

系 11.166 如果 $(R, \mathfrak{m})$ 是诺特局部环, 则 $\text{ht}(\mathfrak{m}) \leqslant \mu(\mathfrak{m})$, 且

$$\dim(R) \leqslant \mu(\mathfrak{m}).$$

证明 如果 $\mu(\mathfrak{m}) = d$, 则 $\mathfrak{m} = (x_1, \cdots, x_d)$. 因 $\mathfrak{m}$ 显然是在它自身上的极小素理想, 定理 11.162, 即广义主理想定理给出 $\text{ht}(\mathfrak{m}) \leqslant d = \mu(\mathfrak{m})$.

如果 $\mathfrak{p} \neq \mathfrak{m}$ 是 R 中的素理想, 则任意素链 $\mathfrak{p} = \mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_h$ 可以加长为长度是 $h+1$ 的素链 $\mathfrak{m} \supsetneq \mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_h$. 所以 $h < \mu(\mathfrak{m})$, 从而 $\dim(R) = \text{ht}(\mathfrak{m}) \leqslant \mu(\mathfrak{m})$. ■

定义 **正则局部环**是指一个诺特局部环 $(R, \mathfrak{m})$ 满足

$$\dim(R) = \mu(\mathfrak{m}).$$

显然每个域都是维数为 0 的正则局部环，每个 DVR 是维数为 1 的正则局部环．从定义并不清楚是否还有其他的例子．即将引入的正则序列的概念使我们能够更好地了解正则局部环．回忆如果 M 是 R-模，则元素 $c \in R$ 称为在 M 上正则如果由 $m \mapsto cm$ 给出的映射 $M \to M$ 是单射，即 $cm = 0$ 蕴涵 $m = 0$．

定义　设 $x_1, \cdots, x_n$ 是交换环 R 中的一个序列，如果 x_1 在 M 上是正则的，x_2 在 $M/(x_1)M$ 上是正则的，x_3 在 $M/(x_1, x_2)M$ 上是正则的，…，x_n 在 $M/(x_1, \cdots, x_{n-1})M$ 上是正则的，则称序列 $x_1, \cdots, x_n$ 为 M-**正则序列**．如果 $M = R$，则也称 $x_1, \cdots, x_n$ 为一个 R-序列．

例如，如果 $R = k[x_1, \cdots, x_n]$ 是域 k 上的多项式环，则易知 $x_1, \cdots, x_n$ 是一个 R-序列．

习题 11.75 给出一个 R-序列的置换不是 R-序列的例子．然而，如果 R 是局部的，则一个 R-序列的每个置换也是 R-序列（见 Bruns-Herzog 所著的《Cohen-Macaulay Rings》，5 页）．

广义主理想定理给出了素理想的高度的上界；下一引理给出一个下界．

引理 11.167　设 R 是交换环．

（i）如果 $x \in R$ 不是零因子，则 x 不在极小素理想中．

（ii）如果 $\mathfrak{p}$ 是 R 中的素理想而 $x \in \mathfrak{p}$ 不是零因子，则

$$\operatorname{ht}(\mathfrak{p}/(x)) + 1 \leqslant \operatorname{ht}(\mathfrak{p}).^{\ominus}$$

（iii）如果 R 中的一个素理想 $\mathfrak{p}$ 包含一个 R-序列 $x_1, \cdots, x_d$，则

$$d \leqslant \operatorname{ht}(\mathfrak{p}).$$

证明　（i）假定相反，$\mathfrak{p}$ 是包含 x 的非零极小素理想．现在 $R_\mathfrak{p}$ 是环，它只有一个非零素理想，就是 $\mathfrak{p}_\mathfrak{p}$，它必是诣零根．于是 $x/1$ 和 $\mathfrak{p}_\mathfrak{p}$ 中的每个元素一样是幂零的．如果在 $R_\mathfrak{p}$ 中 $x^m/1 = 0$，则存在 $\sigma \notin \mathfrak{p}$（从而 $\sigma \neq 0$）使得 $\sigma x = 0$，与 x 不是零因子矛盾．

（ii）如果 $h = \operatorname{ht}(\mathfrak{p}/(x))$，则存在 $R/(x)$ 中的素链：

$$\mathfrak{p}/(x) \supsetneqq \mathfrak{p}_1/(x) \supsetneqq \cdots \supsetneqq \mathfrak{p}_h/(x).$$

把它提升回到 R，有素链 $\mathfrak{p} \supsetneqq \mathfrak{p}_1 \supsetneqq \cdots \supsetneqq \mathfrak{p}_h$ 且 $\mathfrak{p}_h \supseteq (x)$．因 x 不是零因子，（i）说 $\mathfrak{p}_h$ 不是极小素理想．所以存在素理想 $\mathfrak{p}_{h+1}$ 真包含在 $\mathfrak{p}_h$ 中，这表明 $\operatorname{ht}(\mathfrak{p}) \geqslant h + 1$．

（iii）对 $d \geqslant 1$ 用归纳法证明．关于基础步 $d = 1$，假设相反，$\operatorname{ht}(\mathfrak{p}) = 0$；则 $\mathfrak{p}$ 是极小素理想，与（i）矛盾．关于归纳步，（ii）给出 $\operatorname{ht}(\mathfrak{p}/(x_1)) + 1 \leqslant \operatorname{ht}(\mathfrak{p})$．现在根据习题11.79（ii），$\mathfrak{p}/(x_1)$ 包含一个 $(R/(x_1))$-序列 $x_2 + (x_1), \cdots, x_d + (x_1)$，从而归纳假设给出 $d - 1 \leqslant \operatorname{ht}(\mathfrak{p}/(x_1))$．所以（ii）给出 $d \leqslant \operatorname{ht}(\mathfrak{p})$．■

命题 11.168　设 $(R, \mathfrak{m})$ 是诺特局部环．如果 $\mathfrak{m}$ 可以由一个 R-序列 $x_1, \cdots, x_d$ 生成，则 R 是正则局部环且

$$d = \dim(R) = \mu(\mathfrak{m}).$$

注　我们立刻要证明它的逆：在正则局部环中，极大理想可由一个 R-序列生成．

证明　考虑不等式

$$d \leqslant \operatorname{ht}(\mathfrak{m}) \leqslant \mu(\mathfrak{m}) \leqslant d.$$

第一个不等式成立是根据引理 11.167，第二个是根据系 11.166，第三个是根据命题 11.165．由此，

⊖　实际上有等式

$$\operatorname{ht}(\mathfrak{p}/(x)) + 1 = \operatorname{ht}(\mathfrak{p}).$$

所有的不等式事实上都是等式，因为 $\dim(R)=\mathrm{ht}(\mathfrak{m})$，从而得到本命题．■

例 11.169 设 k 是域并设 $R=k[[x_1,\cdots,x_r]]$ 是 r 个变量 $x_1,\cdots,x_r$ 的形式幂级数环．回忆元素 $f\in R$ 是序列

$$f=(f_0,f_1,f_2,\cdots,f_n,\cdots),$$

其中 f_n 是 $k[x_1,\cdots,x_r]$ 中全次数为 n 的齐次多项式，乘法定义为

$$(f_0,f_1,f_2,\cdots)(g_0,g_1,g_2,\cdots)=(h_0,h_1,h_2,\cdots),$$

其中 $h_n=\sum_{i+j=n}f_ig_j$．我们断言 R 是有极大理想 $\mathfrak{m}=(x_1,\cdots,x_r)$ 和剩余域 k 的局部环．首先，$R/\mathfrak{m}\cong k$，从而 $\mathfrak{m}$ 是极大理想．为证明 $\mathfrak{m}$ 是唯一的极大理想，只需证明：如果 $f\in R$ 且 $f\notin\mathfrak{m}$，则 f 是单位．现在 $f\notin\mathfrak{m}$ 当且仅当 $f_0\neq 0$，我们现在证明 f 是单位当且仅当 $f_0\neq 0$．如果 $fg=1$，则 $f_0g_0=1$，从而 $f_0\neq 0$；反之，如果 $f_0\neq 0$，则可以由 $(f_0,f_1,f_2,\cdots)(g_0,g_1,g_2,\cdots)=1$ 递归地解出 g_n，如果定义 $g=(g_0,g_1,g_2,\cdots)$，则有 $fg=1$．

习题 11.83 证明环 R 是诺特环．但 $R/(x_1,\cdots,x_{i-1})$ 同构于 $k[[x_i,\cdots,x_r]]$，所以它是整环，从而 x_i 是 $R/(x_1,\cdots,x_{i-1})$ 上的正则元素．由于 $x_1,\cdots,x_r$ 是一个 R-序列，因此命题 11.168 证明 $R=k[[x_1,\cdots,x_r]]$ 是正则局部环．■

下一引理为归纳法做准备．

引理 11.170 设 $(R,\mathfrak{m},k)$ 是诺特局部环，并设 $x\in\mathfrak{m}-\mathfrak{m}^2$．

（i）如果 $x_1+(x),\cdots,x_s+(x)$ 是 $\mathfrak{m}/x\mathfrak{m}$ 的极小生成集，则 $x_1,\cdots,x_s$ 是 $\mathfrak{m}$ 的极小生成集．

（ii）

$$\mu(\mathfrak{m}/x\mathfrak{m})=\mu(\mathfrak{m})-1.$$

证明 （i）记 $\overline{R}=R/(x)$，$\overline{\mathfrak{m}}=\mathfrak{m}/x\mathfrak{m}$，对一切 $r\in R$，$\overline{r}=r+(x)$．如果 $x_1,\cdots,x_s$ 生成 $\mathfrak{m}$，设 $y\in\mathfrak{m}$．则 $\overline{y}=\sum_i r'_i\overline{x}_i$，其中 $r'_i\in k$．提升到 R 得 $y-\sum_i r_ix_i\in(x)$，其中 $r'_i=r_i+\mathfrak{m}$．所以存在 $r\in R$ 使得 $y=rx+\sum r_ix_i$.

为证明极小性，命题 11.165 说只需证明陪集 $x^*=x+\mathfrak{m}^2$，$x_i^*=x_i+\mathfrak{m}^2$ 形成 $\mathfrak{m}/\mathfrak{m}^2$ 的基．因为 $x,x_1,\cdots,x_s$ 生成 $\mathfrak{m}$，所以这些元素张成 $\mathfrak{m}/\mathfrak{m}^2$．为证明线性无关，假定 $a'x^*+\sum a'_ix_i^*=0$，其中 $a',a'_i\in k$．提升到 R，有

$$ax+\sum a_ix_i\in\mathfrak{m}^2, \tag{8}$$

我们需要证明 $a,a_i\in\mathfrak{m}$（因为在 $k=R/\mathfrak{m}$ 中必有 $a',a'_i=0$）．在 $\overline{R}=R/(x)$ 中，这个关系变成

$$\sum_i\overline{a}_i\overline{x}_i\in\overline{\mathfrak{m}}^2.$$

由于 $\overline{x}_1,\cdots,\overline{x}_s$ 是 $\overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2$ 的基，对一切 i 有 $a'_i=0$；即对一切 $i,a_i\in\mathfrak{m}$．由(8)式，$ax\in\mathfrak{m}^2$．因 $x\notin\mathfrak{m}^2$，所以正如所要的 $a\in\mathfrak{m}$．

（ii）从（i）立即可得．■

引理 11.171 设 $(R,\mathfrak{m})$ 是正则局部环．如果 $x\in\mathfrak{m}-\mathfrak{m}^2$，则 $R/(x)$ 是正则的且 $\dim(R/(x))=\dim(R)-1$．

证明 因 R 是正则的，有 $\dim(R)=\mu(\mathfrak{m})$．先注意 $\dim(R)=\mathrm{ht}(\mathfrak{m})$．我们需要证明 $\mathrm{ht}(\mathfrak{m}^*)=\mu(\mathfrak{m}^*)$，其中 $\mathfrak{m}^*=\mathfrak{m}/(x)$．根据系 11.164，$\mathrm{ht}(\mathfrak{m})\leqslant\mathrm{ht}(\mathfrak{m}^*)+1$．因此，

$$\mathrm{ht}(\mathfrak{m})-1\leqslant\mathrm{ht}(\mathfrak{m}^*)$$

$$\leqslant \mu(\mathfrak{m}^*)$$
$$= \mu(\mathfrak{m}) - 1$$
$$= \mathrm{ht}(\mathfrak{m}) - 1.$$

倒数第二个等式是引理 11.170；最后一个等式成立是因为 R 是正则的．所以 $\dim(R^*) = \mathrm{ht}(\mathfrak{m}^*) = \mu(\mathfrak{m}^*)$，从而 $R^* = R/(x)$ 是正则的且 $\dim(R/(x)) = \dim(R) - 1$． ■

我们现在要证明正则局部环是整环，然后用它证明命题 11.168 的逆．

命题 11.172 *每个正则局部环 $(R,\mathfrak{m})$ 都是整环．*

证明 对 $d = \dim(R)$ 用归纳法证明．如果 $d = 0$，则根据习题 11.78，R 是域．如果 $d > 0$，设 $\mathfrak{p}_1, \cdots, \mathfrak{p}_s$ 是 R 中的极小素理想（根据系 6.120，只有有限个这样的素理想）．如果 $\mathfrak{m} - \mathfrak{m}^2 \subseteq \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_s$，则命题 6.14 给出 $\mathfrak{m} \subseteq \mathfrak{p}_i$，因为 $d = \mathrm{ht}(\mathfrak{m}) > 0$，这是不可能出现的．所以存在 $x \in \mathfrak{m} - \mathfrak{m}^2$ 满足对一切 i，$x \notin \mathfrak{p}_i$．根据引理 11.171，$R/(x)$ 是维数为 $d-1$ 的正则环．归纳假设给出 $R/(x)$ 是整环，因此 (x) 是素理想．由此 (x) 包含一个极小素理想；比如 $\mathfrak{p}_i \subseteq (x)$．

如果 $\mathfrak{p}_i = 0$，则 $\{0\}$ 是素理想且 R 是整环．因此可以假定 $\mathfrak{p}_i \neq \{0\}$．对每个非零 $y \in \mathfrak{p}_i$，存在 $r \in R$ 使得 $y = rx$．因 $x \notin \mathfrak{p}_i$，有 $r \in \mathfrak{p}_i$，从而 $y \in x\mathfrak{p}_i$．于是，$\mathfrak{p}_i \subseteq x\mathfrak{p}_i \subseteq \mathfrak{m}\mathfrak{p}_i$．由于反包含 $\mathfrak{m}\mathfrak{p}_i \subseteq \mathfrak{p}_i$ 恒成立，有 $\mathfrak{p}_i = \mathfrak{m}\mathfrak{p}_i$．现在运用 Nakayama 引理得 $\mathfrak{p}_i = \{0\}$，产生矛盾． ■

命题 11.173 *诺特局部环 $(R,\mathfrak{m},k)$ 是正则的当且仅当 $\mathfrak{m}$ 是由一个 R-序列 $x_1, \cdots, x_d$ 生成的．此外，在这种情形下，*

$$d = \mu(\mathfrak{m}).$$

证明 在命题 11.168 中，我们已经证明了充分性．如果 R 是正则的，则对 $d \geqslant 1$ 用归纳法证明所要的结果，其中 $d = \dim(R)$．基础步成立是因为 R 是整环，从而 x 是正则元素；即 x 不是零因子．关于归纳步，根据引理 11.171，环 $R/(x)$ 是维数为 $d-1$ 的正则环．所以它的极大理想由 $(R/(x))$-序列 $x_1^*, \cdots, x_{d-1}^*$ 生成．根据引理 11.170，$\mathfrak{m}$ 的一个极小生成集是 $x, x_1, \cdots, x_{d-1}$．最后，因为 x 不是零因子，所以根据习题 11.79（i）这是一个 R-序列． ■

我们现在用整体维数来刻画正则局部环．

引理 11.174 *设 $(R,\mathfrak{m},k)$ 是局部环．如果 A 是 R-模且 $pd(A) = n$，又如果 $x \in \mathfrak{m}$ 是 A-正则的，则 $pd(A/xA) = n+1$．*

证明 因 x 是 A-正则的，存在正合列

$$0 \to A \xrightarrow{\mu_x} A \to A/xA \to 0,$$

其中 $\mu_x : a \mapsto xa$．根据引理 11.147，有 $pd(A/xA) \leqslant n+1$．

考虑用 k 作张量积形成的长正合列的一部分：

$$0 = \mathrm{Tor}_{n+1}^R(A,k) \to \mathrm{Tor}_{n+1}^R(A/xA,k) \xrightarrow{\partial} \mathrm{Tor}_n^R(A,k) \xrightarrow{(\mu_x)_*} \mathrm{Tor}_n^R(A,k).$$

现在根据引理 11.155，$pd(A) \leqslant n$ 当且仅当 $\mathrm{Tor}_{n+1}^R(A,k) = \{0\}$，从而第一项是 $\{0\}$．诱导映射 $(\mu_x)_*$ 是乘 x. 然而，如果 $\mu'_x : k \to k$ 是乘 x，则 $x \in \mathfrak{m}$ 蕴涵 $\mu'_x = 0$；所以 $(\mu_x)_* = (\mu'_x)_* = 0$．现在正合性给出 $\partial : \mathrm{Tor}_{n+1}^R(A/xA,k) \to \mathrm{Tor}_n^R(A,k)$ 是同构．因 $pd(A) = n$，有 $\mathrm{Tor}_n^R(A,k) \neq \{0\}$，从而 $\mathrm{Tor}_{n+1}^R(A/xA,k) \neq \{0\}$．所以正如所要的 $pd(A/xA) \geqslant n+1$． ■

命题 11.175 *如果 $(R,\mathfrak{m},k)$ 是正则局部环，则*

$$D(R) = \mu(\mathfrak{m}) = \dim(R).$$

证明 因 R 是正则的，命题 11.173 说 $\mathfrak{m}$ 可以由 R-序列 $x_1,\cdots,x_d$ 生成．对模 $R,R/(x_1)$，$R/(x_1,x_2),\cdots,R/(x_1,\cdots,x_d)=R/\mathfrak{m}=k$ 运用引理 11.174 可知 $pd(k)=d$．根据命题 11.168，$d=\mu(\mathfrak{m})=\dim(R)$．另一方面，定理 11.157（ⅱ）给出 $d=pd(k)=D(R)$． ■

证明命题 11.175 的逆，即有有限整体维数的诺特局部环是正则的比较困难．

引理 11.176 *设 $(R,\mathfrak{m},k)$ 是有有限整体维数的诺特局部环．如果 $\mu(\mathfrak{m})\leqslant D(R)$ 且 $D(R)\leqslant d$，其中 d 是 $\mathfrak{m}$ 中最长 R-序列的长度，则 R 是正则局部环．*

证明 根据系 11.166，$\dim(R)\leqslant\mu(\mathfrak{m})$．根据假设 $\mu(\mathfrak{m})\leqslant D(R)\leqslant d$，而引理 11.167 给出 $d\leqslant\mathrm{ht}(\mathfrak{m})=\dim(R)$．所以 $\dim(R)=\mu(\mathfrak{m})$，因此 R 是局部正则环． ■

设 R 是诺特环，设 M 是有限生成 R-模，并设 I 是满足 $IM\neq M$ 的理想．根据习题 11.82，I 包含一个最长 M-序列（这样的序列常叫做 I 中的**极大 M-序列**）．我们要证明，给定一个理想 I 和一个有限生成 R-模 M，I 中的一切极大 M-序列的长度相等．

定义 *如果 R 是交换环，则非零 R-模 B 的一个**相伴素理想**是指形如 $\mathrm{ann}(b)$ 的素理想，其中 $b\in B$ 是非零元素．*

引理 11.177 *设 B 是诺特环 R 上的非零有限生成模．*

（ⅰ）$\mathcal{F}(B)=\{\mathrm{ann}(b):b\in B$ 且 $b\neq 0\}$ 中的极大元素是 B 的相伴素理想．

（ⅱ）存在 B 的有限个相伴素理想，比如 $\mathfrak{p}_1,\cdots,\mathfrak{p}_s$，使得

$$Z(B)=\mathfrak{p}_1\cup\cdots\cup\mathfrak{p}_s,$$

其中 $Z(B)=\{r\in R$：有某个非零 $b\in B$ 使得 $rb=0\}$．

证明 （ⅰ）因为 R 是诺特环，所以理想的集合 $\mathcal{F}(B)$ 有极大元素．设 $\mathrm{ann}(b)$ 是这样的极大元素．假设 $rs\in\mathrm{ann}(b)$，其中 $r,s\in R$ 而 $r\notin\mathrm{ann}(b)$．现在 $\mathrm{ann}(b)\subseteq\mathrm{ann}(rb)$，这是因为如果 $ub=0$，则 $u(rb)=0$；由极大性，$\mathrm{ann}(b)=\mathrm{ann}(rb)$．因此，$s\in\mathrm{ann}(rb)$ 蕴涵 $s\in\mathrm{ann}(b)$，从而 $\mathrm{ann}(b)$ 是素理想．

（ⅱ）对每个 $r\in Z(B)$，存在非零 $b\in B$ 使得 $rb=0$；即 $Z(B)=\bigcup\limits_{\mathrm{ann}(b)\in\mathcal{F}(B)}\mathrm{ann}(b)$．如果记 $\mathcal{F}(B)$ 中的极大元素的集合为 $\mathfrak{M}$，则 $Z(B)=\bigcup\limits_{\mathfrak{p}\in\mathfrak{M}}\mathfrak{p}$，这是因为每个 $\mathrm{ann}(b)\in\mathcal{F}(B)$ 包含在一个极大元素中．

只需证明 $\mathfrak{M}$ 是有限的．定义 $B'=\langle b:\mathrm{ann}(b)\in\mathfrak{M}\rangle$．现在 B' 是有限生成的，这是因为 R 是诺特环蕴涵有限生成 R-模的每个子模是有限生成的；设 $B'=\langle b_1,\cdots,b_n\rangle$，并记 $\mathrm{ann}(b_i)$ 为 $\mathfrak{p}_i$．假定存在 $\mathfrak{q}=\mathrm{ann}(b_0)\in\mathfrak{M}$，其中对 $i=1,\cdots,n,b_0\neq b_i$．由于 $b_0\in B'$，存在 $r_i\in R$ 使得 $b_0=\sum\limits_i r_ib_i$．由此，如果 $r\in\bigcap\limits_i\mathfrak{p}_i$，则 $rb_0=0$，即 $\bigcap\limits_i\mathfrak{p}_i\subseteq\mathrm{ann}(b_0)=\mathfrak{q}$．因 $\mathfrak{q}$ 是素理想，命题 6.13 给出某个 i 使得 $\mathfrak{p}_i\subseteq\mathfrak{q}$．由于 $\mathfrak{p}_i$ 是 $\mathcal{F}(B)$ 中的极大元素，因此正如所要的 $\mathfrak{q}=\mathfrak{p}_i$． ■

注 *一个 R-模 B 的一切相伴素理想的集合 $\mathrm{Ass}(B)$ 在更深入的讨论中很重要［$\mathfrak{M}$ 可能是 $\mathrm{Ass}(B)$ 的真子集］．例如，它和准素分解有关（见 Matsumura 所著的《Commutative Ring Theory》，39～42 页）．*

下一引理推广了如下的事实：如果 $(m,n)=1$，则 $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{I}_m,\mathbb{I}_n)=\{0\}$．

引理 11.178 *设 R 是交换环，并设 A 和 B 是 R-模．*

（ⅰ）如果 $\mathrm{ann}(A)$ 包含一个 B-正则元素，则 $\mathrm{Hom}_R(A,B)=\{0\}$．

(ii) 反之，设 R 是诺特环，并设 A 和 B 都是有限生成 R-模．如果 $\mathrm{Hom}_R(A,B)=\{0\}$，则 $\mathrm{ann}(A)$ 包含一个 B-正则元素．

证明 (i) 如果 $r\in\mathrm{ann}(A)$，则对一切 $a\in A$，$ra=0$．因此对一切 $f\in\mathrm{Hom}_R(A,B)$，有 $0=f(ra)=rf(a)$．另一方面，如果 r 是 B-正则元素，则 $rf(a)=0$ 蕴涵 $f(a)=0$，因此 $f=0$.

(ii) 假定相反，$\mathrm{ann}(A)$ 不包含 B-正则元素；即 $\mathrm{ann}(A)\subseteq Z(B)$．根据引理 11.177，存在 B 的有限个相伴素理想，比如 $\mathfrak{p}_1,\cdots,\mathfrak{p}_s$，使得 $\mathrm{ann}(A)\subseteq Z(B)=\mathfrak{p}_1\cup\cdots\cup\mathfrak{p}_s$，因此命题 6.14 说存在某个 $\mathfrak{p}=\mathfrak{p}_i$ 使得 $\mathrm{ann}(A)\subseteq\mathfrak{p}$.

假设 $A_\mathfrak{p}=\{0\}$．如果 $A=\langle a_1,\cdots,a_n\rangle$，则根据命题 11.25，存在 $\sigma_i\notin\mathfrak{p}$ 使得 $\sigma_i a_i=0$．因 $\mathfrak{p}$ 是素理想，$\sigma=\sigma_1\sigma_2\cdots\sigma_n\notin\mathfrak{p}$．但 $\sigma\in\mathrm{ann}A=I\subseteq\mathfrak{p}$，这是一个矛盾．所以 $A_\mathfrak{p}\neq\{0\}$.

我们证明 $\mathrm{Hom}_R(A,B)\neq\{0\}$．根据引理 11.32，只需证明 $\mathrm{Hom}_R(A,B)_\mathfrak{p}\cong\mathrm{Hom}_{R_\mathfrak{p}}(A_\mathfrak{p},B_\mathfrak{p})\neq\{0\}$. 于是可以假定 $(R,\mathfrak{p},k)$ 是有极大理想 $\mathfrak{p}$ 和剩余域 k 的局部环．现在存在元素 $b\in B$ 使得 $\mathrm{ann}(b)=\mathfrak{p}$，从而 $\langle b\rangle\cong R/\mathfrak{p}=k$．因此存在非零映射 $\varphi:k\to B$（取 $1\mapsto b$）．因 $A_\mathfrak{p}\neq\{0\}$，Nakayama 引理给出 $A/\mathfrak{p}A\neq\{0\}$．但 $A/\mathfrak{p}A$ 是 k 上的非零向量空间，从而存在非零映射 $A/\mathfrak{p}A\to k$．把这个映射和映射 φ 复合得非零映射 $A\to B$，因此 $\mathrm{Hom}_R(A,B)\neq\{0\}$. ■

引理 11.179 设 R 是交换环，设 A 和 B 都是 R-模，并设 $x_1,\cdots,x_n$ 是 $\mathrm{ann}(A)$ 中的 B-序列．如果 $I=(x_1,\cdots,x_n)$，则

$$\mathrm{Hom}_R(A,B/IB)\cong\mathrm{Ext}_R^n(A,B).$$

证明 对 $n\geqslant 0$ 用归纳法证明．在 $n=0$ 的情形我们定义 $I=\{0\}$，从而基础步成立．现在假定 $x_1,\cdots,x_{n+1}$ 是 $\mathrm{ann}(A)$ 中的 B-序列，$I=(x_1,\cdots,x_{n+1})$，$J=(x_1,\cdots,x_n)$．先注意存在正合列 $0\to B\to B\to B/x_1B\to 0$，这是因为 x_1 是 B 上的正则元素．考虑长正合列的一部分，其中 x_{1*} 是乘 x_1：

$$\mathrm{Ext}_R^n(A,B)\xrightarrow{x_{1*}}\mathrm{Ext}_R^n(A,B)\xrightarrow{\partial}\mathrm{Ext}_R^n(A,B/x_1B)\to\mathrm{Ext}_R^{n+1}(A,B)\xrightarrow{x_{1*}}\mathrm{Ext}_R^{n+1}(A,B).$$

因 $x_1\in\mathrm{ann}(A)$，诱导映射 x_{1*} 是零映射，且存在短正合列

$$0\to\mathrm{Ext}_R^n(A,B)\to\mathrm{Ext}_R^n(A,B/x_1B)\xrightarrow{\partial}\mathrm{Ext}_R^{n+1}(A,B)\to 0.$$

根据归纳法，$\mathrm{Hom}_R(A,B/JB)\cong\mathrm{Ext}_R^n(A,B)$．乘 x_{n+1} 的映射 $B/JB\to B/JB$ 是单射，这是因为 x_{n+1} 是 (B/JB)-正则的，又 $\mathrm{Hom}_R(A,\ )$ 的左正合性证明 $(x_{n+1})_*$ 是单射 $\mathrm{Hom}_R(A,B/JB)\to\mathrm{Hom}_R(A,B/JB)$．另一方面，$(x_{n+1})_*$ 是零映射，这是因为 $x_{n+1}\in\mathrm{ann}(A)$．因此，$\mathrm{Hom}_R(A,B/JB)=\{0\}$，$\mathrm{Ext}_R^n(A,B)=\{0\}$．所以 $\partial:\mathrm{Ext}_R^n(A,B/x_1B)\to\mathrm{Ext}_R^{n+1}(A,B)$ 是同构．根据归纳法，如果 $B'=B/x_1B$，则 $\mathrm{Hom}_R(A,B'/(x_2,\cdots,x_{n+1})B')\cong\mathrm{Ext}_R^n(A,B/x_1B)$．但

$$B'/(x_2,\cdots,x_{n+1})B'\cong(B/x_1B)/(IB/x_1B)\cong B/IB.$$

因此 $\mathrm{Hom}_R(A,B/IB)\cong\mathrm{Ext}_R^n(A,B/x_1B)$．由此正如所要的有 $\mathrm{Hom}_R(A,B/IB)\cong\mathrm{Ext}_R^{n+1}(A,B)$. ■

下面的结果属于里斯．

命题 11.180 设 R 是交换诺特环，B 是有限生成 R-模，I 是满足 $IB\neq B$ 的理想．则 I 中的一切极大 B-序列有相同的长度，比如 g，其中

$$g=\min\{i:\mathrm{Ext}_R^i(R/I,B)\neq\{0\}\}.$$

证明 设 $x_1,\cdots,x_g$ 是 I 中的极大 B-序列．对一切 $i=1,2,\cdots,g$，定义 $I_i=(x_1,\cdots,x_{i-1})$ $(I_1=\{0\})$．现在 x_i 是 (B/I_iB)-正则元素，因为 $\mathrm{ann}(R/I)=I\supseteq I_i$，因此由引理 11.179，

$$\mathrm{Ext}_R^{i-1}(R/I,B) \cong \mathrm{Hom}_R(R/I,B/I_iB) = \{0\}.$$

另一方面，因 $x_1,\cdots,x_g$ 是 I 中的极大 B-序列，理想 I 不包含 (B/IB)-正则元素．于是引理 11.178 给出

$$\mathrm{Ext}_R^{g}(R/I,B) \cong \mathrm{Hom}_R(R/I,B/IB) \neq \{0\}.$$ ■

定义 如果 R 是诺特环，B 是有限生成 R-模，I 是满足 $IB \neq B$ 的理想，则 B 在 I 中的**等级**是指

$$G(I,B) = I \text{ 中极大 } B\text{-序列的长度}.$$

如果 $(R,\mathfrak{m})$ 是诺特局部环，则称 $G(\mathfrak{m},B)$ 为 B 的**深度**：

$$\mathrm{depth}(B) = G(\mathfrak{m},B).$$

引理 11.176 中的数 d 是 $\mathrm{depth}(R)$.

命题 11.181（奥斯兰德-布赫斯包姆） 设 $(R,\mathfrak{m})$ 是诺特局部环，并设 B 是有限生成 R-模且 $pd(B) = n < \infty$，则

$$pd(B) + \mathrm{depth}(B) = \mathrm{depth}(R).$$

证明 对 $n = pd(B) \geqslant 0$ 用归纳法证明．如果 $n = 0$，则 B 是有限生成投射 R-模，从而根据命题 11.23，B 是自由的．因此 $B \cong \sum_{j=1}^{m} R_j$，其中 $R_j \cong R$，从而对一切 q，$\mathrm{Ext}_R^q(k,B) \cong \sum_{j=1}^{m} \mathrm{Ext}_R^q(k,R)$．由此，正如所要的 $\mathrm{depth}(B) = \mathrm{depth}(R)$．

关于归纳步，存在正合列

$$0 \to \Omega \to F \to B \to 0,$$

其中 F 是有限生成自由 R-模．长正合列是

$$\mathrm{Ext}_R^i(k,F) \to \mathrm{Ext}_R^i(k,B) \to \mathrm{Ext}_R^{i+1}(k,\Omega) \to \mathrm{Ext}_R^{i+1}(k,F).$$

根据引理 11.178，$\mathrm{Ext}_R^0(k,F) = \mathrm{Hom}_R(k,F) = \{0\}$；因 F 是自由的，对一切 $i > 0$，$\mathrm{Ext}_R^i(k,F) = \{0\}$．所以对一切 $i \geqslant 0$，$\mathrm{Ext}_R^i(k,B) \cong \mathrm{Ext}_R^{i+1}(k,\Omega)$．由此

$$\mathrm{depth}(\Omega) = \mathrm{depth}(B) + 1.$$

因 $n = pd(B) > 0$，所以 B 不是投射的，从而 $pd(\Omega) = n - 1$．根据归纳法，$pd(\Omega) + \mathrm{depth}(\Omega) = \mathrm{depth}(R)$. 所以，

$$\begin{aligned}\mathrm{depth}(R) &= pd(\Omega) + \mathrm{depth}(\Omega) \\ &= pd(\Omega) + 1 + \mathrm{depth}(\Omega) - 1 \\ &= pd(B) + \mathrm{depth}(B).\end{aligned}$$ ■

系 11.182 如果 $(R,\mathfrak{m})$ 是诺特局部环且有有限整体维数，则

$$D(R) \leqslant \mathrm{depth}(R).$$

证明 根据命题 11.181，对每个有限生成 R-模 M，$pd(M) \leqslant \mathrm{depth}(R)$．但根据定理 11.134，$D(R) = \sup\{pd(M) : M \text{ 是有限生成的}\}$，因此 $D(R) \leqslant \mathrm{depth}(R)$． ■

为完成正则局部环的同调刻画，剩下的是建立引理 11.176 中的第二个不等式：$\mu(\mathfrak{m}) \leqslant D(R)$．回忆定理 11.157 表明 $D(R) = pd(k)$．如果记 $s = \mu(\mathfrak{m})$，我们通过对 k 的科斯居尔（Koszul）复形和 k 的极小分解进行比较来证明 $s \leqslant pd(k)$．我们所展示的只是 Serre 在《Algèbre Locale: Multiplicités》112～116 页中所做的阐述的一个更详尽的形式．

如果 $f: A \to B$ 是 R-模的映射，设 $\overline{f} = f \otimes 1_k : A \otimes_R k \to B \otimes_R k$．回忆用 A 对短正合列 $0 \to \mathfrak{m}$

$\to R \to k \to 0$ 作张量积，易知 $A \otimes_R k \cong A/\mathfrak{m}A$．在这个等同下，$\overline{f}: a + \mathfrak{m}A \mapsto f(a) + \mathfrak{m}B$.

引理 11.183 设 $(R,\mathfrak{m},k)$ 是诺特局部环，设 $f: A \to B$ 是有限生成 R-模的映射，并设 $\overline{f} = f \otimes 1_k$．

（i）$\overline{f}$ 是满射当且仅当 f 是满射．

（ii）如果附加 A 和 B 都是自由 R-模，则 $\overline{f}$ 是单射蕴涵 f 是（分裂）单射．

证明　（i）如果 $\overline{f}$ 是满射，用 k 对正合列 $A \xrightarrow{f} B \to \operatorname{coker} f \to 0$ 作张量积得正合列

$$A \otimes_R k \xrightarrow{\overline{f}} B \otimes_R k \to (\operatorname{coker} f) \otimes_R k \to 0.$$

因 $\overline{f}$ 是满射，$(\operatorname{coker} f) \otimes_R k = \{0\}$. 但 $(\operatorname{coker} f) \otimes_R k \cong \operatorname{coker} f/\mathfrak{m}\operatorname{coker} f$，从而 $\operatorname{coker} f = \mathfrak{m}\operatorname{coker} f$．现在因为 B 是有限生成的，所以 $\operatorname{coker} f$ 是有限生成的，从而 Nakayama 引理给出 $\operatorname{coker} f = \{0\}$；即 f 是满射．

反之，因 $\otimes_R k$ 是右正合的，f 是满射蕴涵 $\overline{f}$ 是满射．

（ii）假定 $\overline{f}$ 是单射．设 $x_1, \cdots, x_t$ 是 A 的基，并对 $i = 1, \cdots, t$ 设 $b_i = f(x_i)$．因 $\overline{f}$ 是单射，元素 $\overline{b}_i = b_i + \mathfrak{m}B$ 在 $B/\mathfrak{m}B$ 中线性无关，因此它们可以扩张为一个基：存在 $c_1, \cdots, c_s \in B$ 使得 $\overline{b}_1, \cdots, \overline{b}_t, \overline{c}_1, \cdots, \overline{c}_s$ 是 $B/\mathfrak{m}B$ 的基．如同命题 11.23 的证明那样，应用 Nakayama 引理可以证明 $b_1, \cdots, b_t, c_1, \cdots, c_s$ 是 B 的基．如果我们定义 $h: B \to A$ 为 $h(b_i) = x_i$ 和 $h(c_j) = 0$，可知 $hf = 1_A$，因此 f 是单射． ■

定义　设 $(R,\mathfrak{m},k)$ 是诺特局部环．如果 R-模的映射 $f: A \to B$ 满足 $\ker f \subseteq \mathfrak{m}A$，则称 f 为**极小的**．

于是引理说，如果 $f: A \to B$ 是极小的，其中 A 和 B 都是秩有限的自由 R-模，则 $\overline{f}: \overline{A} \to \overline{B}$ 是单射蕴涵 f 是单射．

定义　设 $(R,\mathfrak{m},k)$ 是诺特局部环，并设 A 是有限生成 R-模．如果一个自由分解

$$\cdots \to L_2 \xrightarrow{d_2} L_1 \xrightarrow{d_1} L_0 \xrightarrow{d_0} A \to 0$$

对一切 $n \geq 0$ 满足 L_n 都是有限生成的且 $\ker d_n \subseteq \mathfrak{m}L_n$，即一切 d_n 都是极小的，则称该自由分解为**极小分解**．

命题 11.184　设 $(R,\mathfrak{m},k)$ 是诺特局部环．每个有限生成 R-模 A 都有极小分解．

证明　因 A 是有限生成的，它有极小生成集，比如 $\{a_1, \cdots, a_n\}$．设 L_0 是以 $\{e_1, \cdots, e_n\}$ 为基的自由 R-模，并定义 $d_0: L_0 \to A$ 为对一切 i，$d_0(e_i) = a_i$．在命题 11.23 的证明中我们知道 $\ker d_0 \subseteq \mathfrak{m}L_0$，因此 d_0 是极小的．因 R 是诺特环，$\ker d_0$ 是有限生成的，从而这个构造可以迭代．于是，用归纳法可证明存在 A 的极小分解． ■

命题 11.185　设 $(R,\mathfrak{m},k)$ 是诺特局部环，设 A 是有限生成 R-模，并设

$$\cdots \to L_2 \xrightarrow{d_2} L_1 \xrightarrow{d_1} L_0 \xrightarrow{d_0} A \to 0$$

是极小分解．则对一切 $i \geq 0$，

$$\operatorname{Tor}_i^R(A,k) \cong L_i/\mathfrak{m}L_i.$$

所以，

$$\operatorname{rank}(\operatorname{Tor}_i^R(A,k)) = \operatorname{rank}(L_i).$$

证明　从极小分解中删去 A 得复形 $\mathbf{L}_A$；用 k 对 $\mathbf{L}_A$ 作张量积得复形

$$\overline{\mathbf{L}}_A = \cdots \to \overline{L}_2 \xrightarrow{\overline{d}_2} \overline{L}_1 \xrightarrow{\overline{d}_1} \overline{L}_0 \to 0.$$

现在对每个 i, $\operatorname{im}d_{i+1} = \ker d_i \subseteq \mathfrak{m}L_i$ 蕴涵 $\overline{d}_i = 0$，因此对一切 $i \geqslant 0$，$H_i(\overline{\mathbf{L}}_A) \cong \overline{L}_i$．另一方面，$\overline{\mathbf{L}}_A = \mathbf{L}_A \otimes_R k$，因此 Tor 的定义给出 $H_i(\mathbf{L}_A \otimes_R k) = \operatorname{Tor}_i^R(A,k)$．所以 $\operatorname{Tor}_i^R(A,k) \cong \overline{L}_i \cong L_i/\mathfrak{m}L_i$． ■

我们作一个初步考察．如果 $(R,\mathfrak{m},k)$ 是诺特局部环而 M 是 R-模，则我们已经知道 $M/\mathfrak{m}M \cong M \otimes_R k$；记 $M/\mathfrak{m}M$ 为 $\overline{M}$．映射 $\varphi: M \to M'$ 诱导出映射 $\overline{\varphi}: \overline{M} \to \overline{M}'$ 为

$$\overline{\varphi}: u + \mathfrak{m}M \mapsto \varphi(u) + \mathfrak{m}M';$$

如果 φ 满足附加条件 $\operatorname{im}\varphi \subseteq \mathfrak{m}M'$，则存在第二个诱导映射 $\tilde{\varphi}: M/\mathfrak{m}M \to \mathfrak{m}M/\mathfrak{m}^2M$，它由

$$\tilde{\varphi}(u + \mathfrak{m}M) = \varphi(u) + \mathfrak{m}^2M'$$

给出．

引理 11.186 设 $(R,\mathfrak{m},k)$ 是局部环，设 A 是有限生成 R-模，并设

$$\cdots \to L_2 \xrightarrow{d_2} L_1 \xrightarrow{d_1} L_0 \xrightarrow{d_0} A \to 0$$

是 A 的极小分解．如果 $\cdots \to M_2 \xrightarrow{D_2} M_1 \xrightarrow{D_1} M_0 \xrightarrow{\varepsilon} A \to 0$ 是复形满足

（i）每个 M_p 都是有限生成自由 R-模；

（ii）$\overline{\varepsilon}: \overline{M}_0 \to \overline{A}$ 是单射；

（iii）对一切 $p > 0$，有 $D_p(M_p) \subseteq \mathfrak{m}M_{p-1}$，且由 $u_p + \mathfrak{m}M_p \mapsto D_p(u_p) + \mathfrak{m}^2M_{p-1}$ 给出的 $\widetilde{D}_p: \overline{M}_p \to \mathfrak{m}M_{p-1}/\mathfrak{m}^2M_{p-1}$ 是单射；

则对一切 $p \geqslant 0$，$\operatorname{rank}(M_p) \leqslant \operatorname{rank}(L_p) = \operatorname{rank}(\operatorname{Tor}_p^R(A,k))$．

证明 我们要证明每个 M_p 同构于 L_p 的一个直和项．根据定理 10.46，即比较定理，存在映射 f_p 使得下图交换：

$$\begin{array}{ccccccc}
\cdots \to & M_1 & \xrightarrow{D_1} & M_0 & \xrightarrow{\varepsilon} & A & \to 0 \\
& \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_0} & & \downarrow{\scriptstyle 1_A} & \\
\cdots \to & L_1 & \xrightarrow[d_1]{} & L_0 & \xrightarrow[d_0]{} & A & \to 0
\end{array}$$

所以只需找到满射 $g_p: L_p \to M_p$：因 M_p 是自由的，从而是投射的，于是 M_p 就和 L_p 的一个直和项同构．我们断言如果 $\overline{f}_p: \overline{M}_p \to \overline{L}_p$ 是单射，那么就存在这样的映射 g_p．现在 $\overline{M}_p$ 和 $\overline{L}_p$ 都是 k 上的向量空间，因此子空间 $\overline{f}_p(\overline{M}_p) \cong \overline{M}_p$ 是 $\overline{L}_p$ 的直和项；即存在（必然是）满射 $\gamma: \overline{L}_p \to \overline{M}_p$ 使得 $\gamma\overline{f}_p = 1_{\overline{M}_p}$．设 $\pi: M_p \to \overline{M}_p$ 和 $\nu: L_p \to \overline{L}_p$ 是自然映射（认为 $\overline{M}_p = M_p/\mathfrak{m}M_p$ 和 $\overline{L}_p = L_p/\mathfrak{m}L_p$），并考虑图

$$\begin{array}{ccccc}
& & L_p & & \\
& \swarrow{\scriptstyle g_p} & \downarrow{\scriptstyle \gamma\pi} & & \\
M_p & \xrightarrow[\nu]{} & \overline{M}_p & \to & 0
\end{array}$$

因 L_p 是自由的，存在 g_p 使得 $\nu g_p = \gamma\pi$；即 $\overline{g}_p = \gamma\pi$．因此 $\overline{g}_p$ 是满射，从而根据引理 11.183，g_p 是满射．

剩下的是对 $p \geqslant 0$ 用归纳法证明陈述中列出的条件蕴涵每个 $\overline{f}_p$ 都是单射．关于基础步，$d_0 f_0 = \varepsilon$ 蕴涵 $\overline{d}_0\overline{f}_0 = \overline{\varepsilon}$．根据假设，$\overline{\varepsilon}$ 和 $\overline{d}_0$ 都是单射．然而引理11.183（i）证明两者都是同构，这是因为 ε 和 d_0 都是满射．由此 $\overline{f}_0$ 是单射（事实上，它甚至是同构）．

关于归纳步，考虑下面的交换图．

$$\begin{array}{ccc} M_p/\mathfrak{m}M_p & \xrightarrow{\overline{f}_p} & L_p/\mathfrak{m}L_p \\ \downarrow \widetilde{D}_p & & \downarrow \widetilde{d}_p \\ \mathfrak{m}M_{p-1}/\mathfrak{m}^2M_{p-1} & \xrightarrow{\overline{f}_{p-1}} & \mathfrak{m}L_{p-1}/\mathfrak{m}^2L_{p-1} \end{array}$$

因 $\mathbf{L}.$ 是复形，有 $\operatorname{im} d_p \subseteq \ker d_{p-1}$；因 $\mathbf{L}.$ 是极小分解，有 $\ker d_{p-1} \subseteq \mathfrak{m}L_{p-1}$；因此映射 $\widetilde{d}_p$ 有定义．根据归纳假设，$\overline{f}_{p-1}$ 是单射；因此 $\overline{f}_{p-1}\widetilde{D}_p$ 是单射，这是因为根据假设 $\widetilde{D}_p$ 是单射．所以 $\widetilde{d}_p\overline{f}_p$ 是单射，这蕴涵 $\overline{f}_p$ 是单射． ■

我们将看到下面的复形 $\mathbf{M}.$ 满足引理 11.186 中的条件．

定义 设 $x_1,\cdots,x_s$ 是交换环 R 中元素的序列．定义**科斯居尔复形** $\mathbf{M}(x_1,\cdots,x_s).$ 如下：

$$\mathbf{M}(x_1,\cdots,x_s)_p = \bigwedge^p(F),$$

其中 F 是以 $\{e_1,\cdots,e_s\}$ 为基的自由 R-模．定义微分 $D_p: \bigwedge^p(F) \to \bigwedge^{p-1}(F)$ 为

$$D_1\Big(\sum_{i=1}^{s} c_i e_i\Big) = \sum_{i=1}^{s} c_i x_i,$$

其中对一切 i，$c_i \in R$（从而 $D_1(e_i) = x_i$），并对 $p > 1$，

$$D_p(e_{i_1}\wedge\cdots\wedge e_{i_p}) = \sum_{r=0}^{p}(-1)^{r-1}x_r e_{i_1}\wedge\cdots\wedge\hat{e}_{i_r}\wedge\cdots\wedge e_{i_p}.$$

如果 A 是 R-模，定义**科斯居尔复形** $\mathbf{M}(x_1,\cdots,x_s,A).$ 为

$$\mathbf{M}(x_1,\cdots,x_s,A). = A\otimes_R \mathbf{M}(x_1,\cdots,x_s)..$$

我们把 $D_{p-1}D_p = 0$ 的简单计算留给读者，它和引理 10.114 的证明类似．于是科斯居尔复形确实是一个复形．

注意 $\bigwedge^0(F) = R$ 和 $\operatorname{im} d_1 = I$，其中 $I = (x_1,\cdots,x_s)$．一般来说，科斯居尔复形不是无圈的；即它不是一个正合列．然而，如果 $x_1,\cdots,x_s$ 是 R-序列，则增加自然映射 $\varepsilon: \bigwedge^0(F) \to R/I$ 给出 R/I 的自由分解（见 Bruns-Herzog 所著的《Cohen-Macaulay Rings》，49 页）．

考察 $\mathbf{M}(x_1,\cdots,x_s,k).$ 的第 p 项，根据定义它是 $k\otimes_R\bigwedge^p(F)$．因 F 是自由的且秩为 s，从定理 9.140，即二项式定理可知 $\bigwedge^p(F)$ 是自由的且秩为 $\binom{s}{p}$，因此 $k\otimes_R\bigwedge^p(F)$ 是 k 上的 $\binom{s}{p}$ 维向量空间．于是，如果我们如同引理 11.186 那样记 $\bigwedge^p(F)$ 为 M_p，则 $k\otimes_R\bigwedge^p(F)$ 是 $\overline{M}_p$．

如果 $x_1,\cdots,x_s$ 是 $\mathfrak{m}$ 的极小生成集，则命题 11.165 说 $x_1^*,\cdots,x_s^*$ 是 $\mathfrak{m}/\mathfrak{m}^2$ 的基，其中 $x_i^* = x_i + \mathfrak{m}^2$．如果 M 是 R-模，则存在同构 $\mathfrak{m}M/\mathfrak{m}^2M \to (\mathfrak{m}/\mathfrak{m}^2)\otimes_R M$，它由

$$\sum_i x_i v_i + \mathfrak{m}^2 M \mapsto \sum_i x_i^* \otimes v_i$$

给出，其中 $v_i \in M'$．如果 $\varphi: M \to M'$ 有 $\operatorname{im}\varphi \subseteq \mathfrak{m}M'$ 的性质，则 $\varphi(u) = \sum_i x_i v_i'$，其中 $v_i' \in M'$．把 $\widetilde{\varphi}: M/\mathfrak{m}M \to \mathfrak{m}M'/\mathfrak{m}^2M'$ 和上面的同构结合起来使得我们可以认为 $\widetilde{\varphi}: M/\mathfrak{m}M \to (\mathfrak{m}/\mathfrak{m}^2)\otimes_R M'$：

$$\widetilde{\varphi}: u + \mathfrak{m}M \mapsto \varphi(u) + \mathfrak{m}^2 M' = \sum_i x_i v_i' + \mathfrak{m}^2 M' \mapsto \sum_i x_i^* \otimes v_i'.$$

引理 11.187 设 $(R,\mathfrak{m},k)$ 是诺特局部环，并设 $x_1,\cdots,x_s$ 是 $\mathfrak{m}$ 的极小生成集，则科斯居尔复形 $\mathbf{M}(x_1,\cdots,x_s).$ 满足引理 11.186 中的条件．

证明 首先，科斯居尔复形的每个项 $M_p=\bigwedge^p(F)$ 是有限生成自由 R-模．其次，定义 $\varepsilon:R\to k$ 为自然映射．因 $\ker\varepsilon=\mathfrak{m}$，根据引理 11.183，映射 $\bar{\varepsilon}$ 是单射．关于第三个条件，回忆关于 $D_p:\bigwedge^p(F)\to\bigwedge^{p-1}(F)$ 的公式（其中 F 是以 $e_1,\cdots,e_s$ 为基的自由 R-模）：

$$D_p(e_{i_1}\wedge\cdots\wedge e_{i_p})=\sum_{r=1}^{p}(-1)^{r-1}x_r e_{i_1}\wedge\cdots\wedge\hat{e}_{i_r}\wedge\cdots\wedge e_{i_p}.$$

因子 x_r 的出现迫使每个项，从而整个和进入 $\mathfrak{m}M_{p-1}$．

最后，如果 $M_p=\bigwedge^p(F)$ 和 $M_{p-1}=\bigwedge^{p-1}(F)$，我们证明由

$$\widetilde{D}_p(u+\mathfrak{m}M_p)=D_p(u)+\mathfrak{m}^2M_{p-1}$$

给出的 $\widetilde{D}_p:M_p/\mathfrak{m}M_p\to\mathfrak{m}M_{p-1}/\mathfrak{m}^2M_{p-1}$ 是单射．回忆如果 $e_1,\cdots,e_s$ 是自由模 F 的基，则 $M_p=\bigwedge^p(F)$ 的一个基是一切 e_I 的集合，其中 $I=i_1<\cdots<i_p$ 是递增 $p\leqslant s$ 表且 $e_I=e_{i_1}\wedge\cdots\wedge e_{i_p}$．如果 $u=\sum_I\alpha_I e_I$，我们可以假定 α_I 对每个递增表 I 都有定义（某些 α_I 可能是 0）．现在对指标的每个 p 元组 $i_1,\cdots,i_p$（不必递增，且指标可以重复）定义 α_I：如果某个指标是重复的，令 $\alpha_I=0$；如果 I' 是对调 I 中的两个指标得到的，则令 $\alpha_I=-\alpha_{I'}$．用这个记号，我们可以重写 D_p 的公式：

$$\begin{aligned}D_p(u)&=D_p\Big(\sum_I\alpha_I e_I\Big)\\&=\sum_{j=1}^{s}x_j\sum_L\alpha_{jL}e_L,\end{aligned}$$

其中 $L=\ell_1<\cdots<\ell_{p-1}$ 是递增 $p-1\leqslant s$ 表，$jL=j,\ell_1,\cdots,\ell_{p-1}$．注意 α_{jL} 或者是 0，或者是 $\pm\alpha_I$，其中 I 是重排 jL 得到的递增表．现在假定 $u=\sum_I\alpha_I e_I\notin\mathfrak{m}M_p$；即在 $M_p/\mathfrak{m}M_p$ 中，$u+\mathfrak{m}M_p\neq 0$．因各个 e_I 是 M_p 的基，必有某个 $\alpha_I\notin\mathfrak{m}$；即 α_I 是 R 中的单位．如果 $I=i_1<\cdots<i_p$，定义 $j=i_1$ 和 $L=i_2<\cdots<i_p$．e_L 的系数 $\alpha_{jL}=\alpha_I$ 不在 $\mathfrak{m}$ 中，因此在 M_{p-1} 中 $\sum_L\alpha_{jL}e_L\neq 0$（因为各个 e_L 形成 M_{p-1} 的基）．在同构 $\mathfrak{m}M_{p-1}/\mathfrak{m}^2M_{p-1}\to(\mathfrak{m}/\mathfrak{m}^2)\otimes_R M_{p-1}$ 下，

$$\widetilde{D}_p(u)=\sum_{j=1}^{s}x_j^*\otimes\sum_L\alpha_{jL}e_L,$$

其中 $x_j^*=x_j+\mathfrak{m}$．因 $x_1^*,\cdots,x_s^*$ 是 $\mathfrak{m}/\mathfrak{m}^2$ 的基，一个元素 $\sum_j x_j^*\otimes v_j=0$ 当且仅当每个 $v_j=0$．所以，如果 $u\notin\mathfrak{m}M_p$，则 $\widetilde{D}_p(u+\mathfrak{m}M_p)\neq 0$，因此 $\widetilde{D}_p$ 是单射． ■

命题 11.188 如果 $(R,\mathfrak{m},k)$ 是整体维数 $D(R)$ 有限的诺特局部环，则

$$\mu(\mathfrak{m})\leqslant D(R).$$

证明 设 $s=\mu(\mathfrak{m})$，并设 $\{x_1,\cdots,x_s\}$ 是 $\mathfrak{m}$ 的极小生成集，则根据引理 11.186，

$$\operatorname{rank}(\mathbf{M}(x_1,\cdots,x_s)_p)\leqslant\operatorname{rank}(\operatorname{Tor}_p^R(k,k)).$$

现在 $\mathbf{M}(x_1,\cdots,x_s)_p=\bigwedge^p(F)$，其中 F 是以 $e_1,\cdots,e_s$ 为基的自由 R-模，因此 $\operatorname{rank}(\mathbf{M}(x_1,\cdots,x_s)_p)=\operatorname{rank}\big(\bigwedge^p(F)\big)=\binom{s}{p}$ 和

$$\binom{s}{p}\leqslant\operatorname{rank}(\operatorname{Tor}_p^R(k,k)).$$

所以 $1 \leqslant \operatorname{rank}(\operatorname{Tor}_s^R(k,k))$，从而 $\operatorname{Tor}_s^R(k,k) \neq \{0\}$. 但引理 11.155 给出

$$pd(k) = \max\{p : \operatorname{Tor}_p^R(k,k) \neq \{0\}\},$$

因此根据系 11.156，$s \leqslant pd(k) = D(R)$. ■

定理 11.189 (塞尔) 诺特局部环 R 是正则的当且仅当 $D(R)$ 有限.

证明 引理 11.176 中这个定理简化为验证两个不等式. 这两个不等式在系 11.182 和命题 11.188 中已经证明. ■

系 11.190 如果 R 是正则局部环，又如果 $\mathfrak{p}$ 是 R 中的素理想，则 $R_\mathfrak{p}$ 也是正则局部环.

证明 因 $\mathfrak{p}$ 是素理想，局部化 $R_\mathfrak{p}$ 是局部环；因为 R 是诺特环，它也是诺特环. 在命题 11.154 中，我们知道 $D(R) \geqslant D(R_\mathfrak{p})$. 所以根据塞尔定理，$R_\mathfrak{p}$ 是正则局部环. ■

我们现在证明每个正则局部环都是 UFD，先从几个初等引理开始.

引理 11.191 如果 R 是诺特整环，则 R 是 UFD 当且仅当高度为 1 的每个素理想都是主理想.

证明 设 R 是 UFD，并设 $\mathfrak{p}$ 是高度为 1 的素理想. 如果 $a \in \mathfrak{p}$ 非零，则 $a = p_1^{e_1} \cdots p_n^{e_n}$，其中 p_i 是不可约的且 $e_i \geqslant 1$. 因 $\mathfrak{p}$ 是素的，必有一个因子，比如 $p_j \in \mathfrak{p}$. 当然 $Rp_j \subseteq \mathfrak{p}$. 但根据命题 6.17，$Rp_j$ 是素理想，因为 $\operatorname{ht}(\mathfrak{p}) = 1$，所以 $Rp_j = \mathfrak{p}$.

反之，因 R 是诺特环，引理 6.18 表明 R 中的每个非零非单位元素都是不可约元素的积，从而命题 6.17 说这已足以证明对每个不可约元素 $\pi \in R$，$R\pi$ 是素理想. 选取在 $R\pi$ 上极小的素理想 $\mathfrak{p}$. 根据主理想定理，即定理 11.161，有 $\operatorname{ht}(\mathfrak{p}) = 1$，因此命题假设给出对某个 $a \in R$ 有 $\mathfrak{p} = Ra$. 所以有某个 $u \in R$ 使得 $\pi = ua$. 因 π 是不可约的，u 必是单位，因此，正如所要的 $R\pi = Ra = \mathfrak{p}$. ■

引理 11.192 设 R 是诺特整环，设 $x \in R$ 是非零元素且 Rx 是素理想，记 $S^{-1}R$ 为 R_x，其中 $S = \{x^n : n \geqslant 0\}$. 则 R 是 UFD 当且仅当 R_x 是 UFD.

证明 必要性的证明留给读者作为练习. 关于充分性，假定 R_x 是 UFD. 设 $\mathfrak{p}$ 是 R 中高度为 1 的素理想. 如果 $x \in \mathfrak{p}$，则 $Rx \subseteq \mathfrak{p}$，又因 $\operatorname{ht}(\mathfrak{p}) = 1$，必有 $Rx = \mathfrak{p}$(因为 Rx 是素理想)，所以在这种情形下 $\mathfrak{p}$ 是主理想. 我们现在可以假定 $x \notin \mathfrak{p}$；即 $S \cap \mathfrak{p} = \varnothing$. 由此，$\mathfrak{p}R_x$ 是 R_x 中高度为 1 的素理想，因此根据假设它是主理想. 因为 x 是 R_x 中的单位，存在某个 $a \in \mathfrak{p}$ 和 $n \geqslant 0$ 使得 $\mathfrak{p}R_x = R_x(a/x^n) = R_x a$. 我们可以假定 $a \notin Rx$. 如果 $a = a_1 x$ 和 $a_1 \notin Rx$，则因 $R_x a = R_x a_1$，可以用 a_1 替换 a. 如果 $a_1 = a_2 x$ 和 $a_2 \notin Rx$，则因 $R_x a_1 = R_x a_2$，可以用 a_2 替换 a_1. 如果这个过程不终止，则对一切 $m \geqslant 1$，存在等式 $a_m = a_{m+1} x$，这就形成一个递增序列 $Ra_1 \subseteq Ra_2 \subseteq \cdots$. 因 R 是诺特环，有某个 m 使得 $Ra_m = Ra_{m+1}$. 因此有某个 $r \in R$ 使得 $a_{m+1} = ra_m$ 和 $a_m = a_{m+1}x = ra_m x$. 因 R 是整环，$1 = rx$；于是 x 是单位，与 Rx 是素理想（因此是真理想）矛盾. 显然 $Ra \subseteq \mathfrak{p}$；我们断言 $Ra = \mathfrak{p}$. 如果 $b \in \mathfrak{p}$，则在 R_x 中 $b = (r/x^m)a$，其中 $r \in R$ 和 $m \geqslant 0$. 因此在 R 中 $x^m b = ra$. 选取 m 极小. 如果 $m > 0$，则 $ra = x^m b \in Rx$；因 Rx 是素理想，或者 $r \in Rx$ 或者 $a \in Rx$. 但因 $S \cap \mathfrak{p} = \varnothing$，所以 $a \notin Rx$，从而 $r = xr'$. 由于 R 是整环，这给出 $r'a = x^{m-1}b$，与 m 的极小性矛盾. 由此可知 $m = 0$，因此 $\mathfrak{p} = Ra$ 是主理想. 现在引理 11.191 证明 R 是 UFD. ■

下面的初等引理当局部化理想是素理想时为真，然而我们只用到理想是极大的情形.

引理 11.193 设 R 是整环，并设 I 是 R 中的非零投射理想. 如果 $\mathfrak{m}$ 是 R 中的极大理想，则

$$I_\mathfrak{m} \cong R_\mathfrak{m}.$$

证明 因 I 是投射 R-模，$I_\mathfrak{m}$ 是投射 $R_\mathfrak{m}$-模. 然而，由于 $R_\mathfrak{m}$ 是局部环，$I_\mathfrak{m}$ 是自由 $R_\mathfrak{m}$-模. 但 $I_\mathfrak{m}$ 是整环 $R_\mathfrak{m}$ 中的理想，因此它必是主理想；即 $I_\mathfrak{m} \cong R_\mathfrak{m}$. ■

定理 11.194（奥斯兰德-布赫斯包姆） *每个正则局部环 R 都是 UFD.*

证明（卡普兰斯基） 对克鲁尔维数 $\dim(R)$ 用归纳法证明，$n=0$（R 是域）和 $n=1$（R 是 DVR）的情形是显然的（见系 11.78）．关于归纳步，选取 $x\in\mathfrak{m}-\mathfrak{m}^2$．根据引理 11.171，$R/Rx$ 是正则局部环且 $\dim(R/Rx)<\dim(R)$；根据命题 11.172，R/Rx 是整环，从而 Rx 是素理想．根据引理 11.192，只需证明 R_x 是 UFD（其中 $R_x=S^{-1}R, S=\{x^n:n\geqslant 0\}$）．设 $\mathfrak{P}$ 是 R_x 中高度为 1 的素理想；我们需要证明 $\mathfrak{P}$ 是主理想．定义 $\mathfrak{p}=\mathfrak{P}\cap R$（因 R 是整环，$R_x\subseteq\operatorname{Frac}(R)$，因此这个交有意义）．因 R 是正则局部环，$D(R)<\infty$，从而 R-模 $\mathfrak{p}$ 有长度有限的自由分解：

$$0\to F_n\to F_{n-1}\to\cdots\to F_0\to\mathfrak{p}\to 0.$$

用 R_x 作张量积，R_x 是一个平坦 R-模（定理 11.28），得到 $\mathfrak{P}$ 的自由 R_x-分解（因为 $\mathfrak{P}=R_x\mathfrak{p}$）：

$$0\to F'_n\to F'_{n-1}\to\cdots\to F'_0\to\mathfrak{P}\to 0, \tag{9}$$

其中 $F'_i=R_x\otimes_R F_i$．

我们断言 $\mathfrak{P}$ 是投射的．根据命题 11.154，只需证明每个局部化 $\mathfrak{P}_{\mathfrak{M}}$ 是投射的，其中 $\mathfrak{M}$ 是 R_x 中的极大理想．现在 $(R_x)_{\mathfrak{M}}$ 是 R 的局部化，因此根据系 11.190，它是正则局部环；它的维数比 $D(R)$ 小，所以根据归纳假设它是 UFD. 现在在 UFD $(R_x)_{\mathfrak{M}}$ 中高度为 1 的素理想 $\mathfrak{P}_{\mathfrak{M}}$ 是主理想．但整环中的主理想是自由的，因此是投射的，从而 $\mathfrak{P}_{\mathfrak{M}}$ 是投射的．所以 $\mathfrak{P}$ 是投射的．

正合列（9）可“因子分解”为分裂短正合列．因 $\mathfrak{P}$ 是投射的，有 $F'_0\cong\mathfrak{P}\oplus\Omega_0$，其中 $\Omega_0=\ker(F'_0\to\mathfrak{P})$．于是 Ω_0 是投射的，它是自由模的直和项，因此 $F'_1\cong\Omega_1\oplus\Omega_0$，其中 $\Omega_1=\ker(F'_1\to F'_0)$．一般地，对一切 $i\geqslant 1$，$F'_i\cong\Omega_i\oplus\Omega_{i-1}$．因此，

$$F'_0\oplus F'_1\oplus\cdots\oplus F'_n\cong(\mathfrak{P}\oplus\Omega_0)\oplus(\Omega_1\oplus\Omega_0)\oplus\cdots.$$

因局部环上的投射模是自由的，可知存在有限生成自由 R_x-模 Q 和 Q' 使得

$$Q\cong\mathfrak{P}\oplus Q'.$$

回忆 $\operatorname{rank}(Q)=\dim_K(K\otimes_{R_x}Q)$，其中 $K=\operatorname{Frac}(R_x)$；现在 $\operatorname{tank}(\mathfrak{P})=1$，又比如 $\operatorname{rank}(Q')=r$，因此 $\operatorname{rank}(Q)=r+1$．

我们仍然需要证明 $\mathfrak{P}$ 是主理想．现在

$$\bigwedge^{r+1}(Q)\cong\bigwedge^{r+1}(\mathfrak{P}\oplus Q').$$

因 Q 是自由的，秩为$r+1$，定理 9.140，即二项式定理给出 $\bigwedge^{r+1}(Q)\cong R_x$．另一方面，定理 9.143 给出

$$\bigwedge^{r+1}(\mathfrak{P}\oplus Q')\cong\sum_{i=0}^{r+1}\Big(\bigwedge^{i}(\mathfrak{P})\otimes_{R_x}\bigwedge^{r+i-1}(Q')\Big). \tag{10}$$

我们断言对一切 $i>1$，$\bigwedge^i(\mathfrak{P})=\{0\}$. 根据引理 11.193，对 R_x 中的每个极大理想 $\mathfrak{M}$ 有 $\mathfrak{P}_{\mathfrak{M}}\cong(R_x)_{\mathfrak{M}}$．现在习题 11.24 给出，对一切极大理想 $\mathfrak{M}$ 和一切 i，

$$\Big(\bigwedge^i(\mathfrak{P})\Big)_{\mathfrak{M}}\cong\bigwedge^i(\mathfrak{P}_{\mathfrak{M}})\cong\bigwedge^i((R_x)_{\mathfrak{M}}).$$

但对一切 $i>1$，$\bigwedge^i((R_x)_{\mathfrak{M}})=\{0\}$（由二项式定理，或更简单地由系 9.138)，因此命题 11.31 对一切 $i>1$ 给出 $\bigwedge^i(\mathfrak{P})=\{0\}$．

我们已经知道（10）中的大多数项都是$\{0\}$，残存的是

$$\bigwedge^{r+1}(\mathfrak{P}\oplus Q')\cong\Big(\bigwedge^0(\mathfrak{P})\otimes_{R_x}\bigwedge^{r+1}(Q')\Big)\oplus\Big(\bigwedge^1(\mathfrak{P})\otimes_{R_x}\bigwedge^{r}(Q')\Big).$$

但 $\bigwedge^{r+1}(Q')=\{0\}$和 $\bigwedge^{r}(Q')\cong R_x$，这是因为 Q' 是自由的，秩为 r. 所以 $\bigwedge^{r+1}(\mathfrak{P}\oplus Q')\cong\mathfrak{P}$. 因 $\mathfrak{P}\cong\bigwedge^{r+1}(\mathfrak{P}\oplus Q')\cong\bigwedge^{r+1}(Q)\cong R_x$，有 $\mathfrak{P}\cong R_x$ 是主理想. 于是 R_x，且因此 R 是 UFD. ■

我们已经研究了局部化，现在简短地转到整体化，并且只描述它的设置. 对于给定的交换诺特环 R，我们已经把它和一族局部环 $R_\mathfrak{p}$ 联系起来，对每个素理想 $\mathfrak{p}$ 有一个 $R_\mathfrak{p}$. 局部环比一般的环简单；例如，如果 R 是戴得金环，它的局部化是一切主理想整环. 整体化是问如何利用一切局部化来收集信息. 考虑不相交并

$$E(R)=\bigcup_{\mathfrak{p}\in\mathrm{Spec}(R)}R_\mathfrak{p}.$$

我们称 $R_\mathfrak{p}$ 为 R 在 $\mathfrak{p}$ 上的**茎**，并定义**投射** $\pi:E(R)\to\mathrm{Spec}(R)$ 为如果 $e\in R_\mathfrak{p}$，则 $\pi(e)=\mathfrak{p}$，即 π 把 $\mathfrak{p}$ 上的茎中的每个点送到 $\mathfrak{p}$ 中.[⊖] 每个元素 $a\in R$ 定义了一个函数 $s_a:\mathrm{Spec}(R)\to E(R)$ 为

$$s_a:\mathfrak{p}\mapsto a/1\in R_\mathfrak{p}.$$

注意 $\pi s_a=1_{\mathrm{Spec}(R)}$. 我们断言不同的元素 $a,b\in R$ 给出不同的函数：即如果 $s_a=s_b$，则 $a=b$. 设 $I=R(a-b)$. 如果对每个素理想 $\mathfrak{p}$，在 $R_\mathfrak{p}$ 中 $(a-b)/1=0$，则对每个 $\mathfrak{p}$，$I_\mathfrak{p}=\{0\}$. 运用命题 11.31 可证明 $a=b$（事实上，这个命题只要求对一切极大理想 $\mathfrak{m}$ 有 $I_\mathfrak{m}=\{0\}$）. 于是可以把任意交换环 R 的元素看作 $\mathrm{Spec}(R)$ 上取值于 $E(R)$ 的函数.

考虑这样的问题：给定 $f\in R_\mathfrak{p}$ 和 $g\in R_\mathfrak{q}$，是否存在 $a\in R$ 使得 $f=a/1\in R_\mathfrak{p}$ 和 $g=a/1\in R_\mathfrak{q}$? 即是否存在 $a\in R$ 使得 $s_a(\mathfrak{p})=f$ 和 $s_a(\mathfrak{q})=g$? 一个“好”的答案或许是：如果 $\mathfrak{p}$ 和 $\mathfrak{q}$ 是互“闭”的，则存在这样的元素 $a\in R$. 由此考虑 $X=\mathrm{Spec}(R)$ 上的一个拓扑或许是重要的，而扎里斯基拓扑是一个好的候选者（子集 $F\subseteq\mathrm{Spec}(R)$ 是闭的如果它满足下面的条件：如果 $\mathfrak{q}\in F$，则只要 $\mathfrak{p}$ 是素理想且 $\mathfrak{q}\subseteq\mathfrak{p}$，就有 $\mathfrak{p}\in F$）. 当然，一旦对 $\mathrm{Spec}(R)$ 确定了一个拓扑，则希望 $E(R)$ 也被拓扑化，而且这些重要的函数应该是连续的.

扎里斯基拓扑和欧几里得空间上的拓扑有很大的不同，它不仅不是一个度量空间（即没有定义两点之间的距离），而且单点子集未必是闭集；例如，$\{\mathfrak{p}\}$ 是闭的当且仅当 $\mathfrak{p}$ 是极大理想. 尽管如此，一个函数 $f:X\to Y$ 的**连续性**仍可定义：f 是连续的，如果对每个开子集 $V\subseteq Y$，$f^{-1}(V)$ 是 X 上的开子集. 等价地，f 是连续的当且仅当对 Y 中的每个闭子集 C，子集 $f^{-1}(C)$ 是 X 的闭子集. 类似地，可以对任意拓扑空间定义紧性的概念（如果 $\{F_i:i\in I\}$ 是一族闭子集，则存在它们之中的有限个闭子集，比如 $F_{i_1},\cdots,F_{i_n}$，使得 $\bigcap_{i\in I}F_i=\bigcap_{j=1}^{n}F_{i_j}$）和连通性的概念（不是两个非空不相交闭子集的并）.

我们提一下一个初等的**粘合**结果. 假设 X 和 Y 都是拓扑空间，$\{U_i:i\in I\}$ 是 X 的一族开子集，$\{f_i:U_i\to Y\}$ 是一族连续函数. 如果这些函数在重叠部分一致，即如果对一切 $i,j\in I$，$f_i\mid(U_i\cap U_j)=f_j\mid(U_i\cap U_j)$，则有唯一的连续函数 $f:\bigcup_i U_i\to Y$ 使得对一切 i 有 $f\mid U_i=f_i$. 这使你想起了正向极限吗?

⊖ 有可能产生混淆，因为对 $\mathfrak{p}$ 有两种看法：看作素理想——R 的一个子集；看作 $\mathrm{Spec}(R)$ 中的一个点. 为区别这两种看法，当把 $\mathfrak{p}$ 看作 $X=\mathrm{Spec}(R)$ 的一个点的时候，常写作 $\mathfrak{p}_x$. 于是，投射 π 定义为对一切 $e\in R_\mathfrak{p}$，$\pi(e)=\mathfrak{p}_x$.

从这个观点出发，可以给出层的正式定义，还有一个运用（第 7 章引入的）预层的等价形式，我们在后面描述．

定义 如果 E 和 X 都是拓扑空间，设 $\pi: E \to X$ 是连续满射．如果 $\mathcal{F} = (E, X, \pi)$ 满足

（ⅰ）π 是**局部同胚**：对每个 $e \in E$，存在包含 e 的开集 U 使得 $\pi(U)$ 是 X 的开子集且 $\pi \mid U$ 是从 U 到 $\pi(U)$ 的同胚．㊀

（ⅱ）对 $x \in X$，E 的子集 $\mathcal{F}_x = \pi^{-1}(x)$ 叫做$\mathcal{F}$的**茎**，且每个 $\mathcal{F}_x$ 都是阿贝尔群．

（ⅲ）如果 $E+E$ 是 $E \times E$ 的子集，它由满足 $\pi(a) = \pi(b)$ 的一切 (a,b) 组成，则由 $(a,b) \mapsto a+b$ 和 $(a,b) \mapsto a-b$ 给出的映射 $E+E \to E$ 都是连续的．

则称 $\mathcal{F} = (E, X, \pi)$ 是一个**阿贝尔群层**．

忽略茎上的代数结构，读者可以认为它是覆盖空间中出现的基本成分．

回忆上面提到的函数 $s_a: \mathrm{Spec}(R) \to E(R)$，下面的概念是重要的．

定义 如果 $\mathcal{F} = (E, X, \pi)$ 是阿贝尔群层，又如果 U 是 X 的开子集，则 U 上的一个**截面**是指一个连续函数 $s: U \to E$ 满足 $\pi s = 1_U$．我们记

$$\Gamma(U, \mathcal{F}) = \{\text{一切截面 } s: U \to E\}.$$

整体截面是指 $\Gamma(X, \mathcal{F})$ 中的截面．

容易验证 $\Gamma(U, \mathcal{F})$ 是阿贝尔群．如果 $V \subseteq U$ 是 X 的开子集，则存在**限制映射**

$$\rho_V^U: \Gamma(U, \mathcal{F}) \to \Gamma(V, \mathcal{F}),$$

它由 $s \mapsto s \mid V$ 给出．此外，函数 ρ_V^U 是同态．

对固定的 $x \in X$，设

$$I(x) = \{\text{包含 } x \text{ 的开集 } U \subseteq X\}.$$

易知 $I(x)$ 在反包含下是偏序集：

$$U \leq V \text{ 意味着 } U \supseteq V.$$

事实上，$I(x)$ 是一个有向指标集，如果给定 $U, V \in I(x)$，则 $U \cap V \in I(x)$，$U \cap V \subseteq U$ 和 $U \cap V \subseteq V$；即 $U \leq U \cap V$ 和 $V \leq U \cap V$．我们可以从截面得到茎．设 $\mathcal{F} = (E, X, \pi)$ 是阿贝尔群层．对每个 $x \in X$，

$$\mathcal{F}_x \cong \varinjlim_{U \in I(x)} \Gamma(U, \mathcal{F}).$$

如果 X 是拓扑空间，则它的开集族（以子集的包含映射作为态射）是一个范畴，记为 **Open**(X)．现在可以定义阿贝尔群的预层．事实上，存在取值于任意范畴中的预层，比如交换环的模，而不只是 **Ab**.

定义 如果 X 是拓扑空间而$\mathcal{C}$是范畴，则 X 上取值于$\mathcal{C}$的**预层**是指一个反变函子 $\mathcal{F}$：**Open**$(X) \to \mathcal{C}$．

如果进一步假定上面提到的粘合结果的一个形式，则层可以由它的截面的预层来构造．

给定一个交换环 R，R-模的层定义为它的茎是 $R_{\mathfrak{p}}$-模，其中 $\mathfrak{p} \in \mathrm{Spec}(R)$．这些层形成有足够的单射的阿贝尔范畴，即每个层可以作为子层嵌入一个内射层．此外，整体截面 $\Gamma(X, \ )$ 是一个左正合函子，层的上同调定义为 $\Gamma(X, \ )$ 的导函子．这些上同调群提供了整体化最重要的方法．关于一个清晰的讨论，我们推荐 J.-P. Serre 的论文，Faisceaux Algèbriques Cohérents，*Annals of Math.* (61) 1955，197～278 页．

㊀ 同胚是双射 $f: X \to Y$，其中 X 和 Y 都是拓扑空间，满足 f 和 f^{-1} 都是连续的．

习题

11.75 设 $R = k[x,y,z]$，其中 k 是域．

(i) 证明 $x, y(1-x), z(1-x)$ 是一个 R-序列．

(ii) 证明 $y(1-x), z(1-x), x$ 不是 R-序列．

11.76 设 R 是交换环．证明 R 中的素理想 $\mathfrak{p}$ 在理想 I 上极小当且仅当在 R/I 中有 $\mathrm{ht}(\mathfrak{p}/I) = 0$．

11.77 如果 $(R,\mathfrak{m},k)$ 是诺特局部环，又如果 B 是有限生成 R-模，证明

$$\mathrm{depth}(B) = \min\{i : \mathrm{Ext}_R^i(k,B) \neq \{0\}\}.$$

11.78 设 R 是正则局部环．

(i) 证明 R 是域当且仅当 $\dim(R) = 0$．

(ii) 证明 R 是 DVR 当且仅当 $\dim(R) = 1$．

11.79 (i) 设 $(R,\mathfrak{m})$ 是诺特局部环，并设 $x \in R$ 是正则元素，即 x 不是零因子．如果 $x_1+(x),\cdots,x_s+(x)$ 是 $(R/(x))$-序列，证明 $x,x_1,\cdots,x_s$ 是 R-序列．

(ii) 设 R 是交换环．如果 $x_1,\cdots,x_d$ 是 R-序列，证明陪集 $x_2+(x_1),\cdots,x_d+(x_1)$ 形成 $(R/(x_1))$-序列．

11.80 设 R 是诺特（交换）环，且有雅各布森根 $J = J(R)$．如果 B 是有限生成 R-模，证明

$$\bigcap_{n\geqslant 1} J^n B = \{0\}.$$

由此推出，如果 $(R,\mathfrak{m})$ 是诺特局部环，则 $\bigcap_{n\geqslant 1}\mathfrak{m}^n B = \{0\}$．

提示：设 $D = \bigcap_{n\geqslant 1} J^n B$，考察 $JD = D$，并用 Nakayama 引理．

11.81 用里斯引理证明命题 11.175 的较弱形式：如果 $(R,\mathfrak{m})$ 是正则局部环，则 $D(R) \geqslant \mu(\mathfrak{m}) = \dim(R)$．

提示：如果 $\mathrm{Ext}_R^d(k,R) \neq \{0\}$，则 $D(R) > d-1$；即 $D(R) \geqslant d$．

设 $\mathfrak{m} = (x_1,\cdots,x_d)$，其中 $x_1,\cdots,x_d$ 是 R-序列，则

$$\begin{aligned}\mathrm{Ext}_R^d(k,R) &\cong \mathrm{Ext}_{R/(x_1)}^{d-1}(k,R/(x_1)) \\ &\cong \mathrm{Ext}_{R/(x_1,x_2)}^{d-2}(k,R/(x_1,x_2)) \cong \cdots \\ &\cong \mathrm{Ext}_k^0(k,k) \cong \mathrm{Hom}_k(k,k) \cong k \neq \{0\}.\end{aligned}$$

11.82 设 R 是交换环，设 M 是有限生成 R-模，并设 I 是满足 $IM \neq M$ 的理想．

(i) 如果 $x_1,x_2,\cdots,x_n$ 是包含在 I 中的 M-序列，证明

$$(x_1) \subsetneq (x_1,x_2) \subsetneq \cdots \subsetneq (x_1,\cdots,x_n).$$

(ii) 如果 R 是诺特环，证明存在包含在 I 中的最长 M-序列．

11.83 如果 k 是域，证明 $k[[x_1,\cdots,x_n]]$ 是诺特环．

提示：定义非零形式幂级数 $f = (f_0,f_1,f_2,\cdots)$ 的阶 $o(f)$ 为满足 $f_n \neq 0$ 的最小 n. 寻找类似于希尔伯特基定理的证明．（见 Zariski-Samuel 所著的《Commutative Algebra II》，138 页．）

11.84 如果 k 是域，证明形式幂级数 $k[[x_1,\cdots,x_n]]$ 的环是 UFD.

附录　选择公理和佐恩引理

今日大多数数学家接受属于 E. Zermelo 和 A. Fraenkel 的集合论的 **ZFC** 公理化；字母 C 是选择（choice）的缩写．运用这个公理化的结果，可以证明选择公理、良序原则和佐恩引理的等价性．我们先回忆第 6 章中的一些定义．

定义　如果 A 是集合，令 $\mathcal{P}(A)^{\#}$ 表示它的一切非空子集的族．**选择公理**陈述为：如果 A 是非空集合，则存在函数 $\beta: \mathcal{P}(A)^{\#} \to A$ 使得对 A 的每个非空子集 $S, \beta(S) \in S$. 这样的函数 β 叫做**选择函数**.

非正式地说，选择公理看起来是一个无害的陈述；它说可以从一个集合的每个非空子集中同时选取一个元素．现在证明选择公理等价于一个我们不愿意它是伪的陈述．

命题 A.1　选择公理成立当且仅当非空集合的笛卡儿积 $\prod_{i \in I} X_i$ 非空．[⊖]

证明　假定选择公理成立．回忆 $\prod_{i \in I} X_i$ 的元素是 I 元组 $x = (x_i)$，其中对一切 $i \in I, x_i \in X_i$. 现在 I 元组实际上是一个函数

$$f: I \to A = \bigcup_{i \in I} X_i,$$

其中对一切 $i \in I, f(i) = x_i \in X_i$．定义 $\varphi: I \to \mathcal{P}(A)^{\#}$ 为 $\varphi(i) = X_i$．如果 $\beta: \mathcal{P}(A)^{\#} \to A$ 是选择函数，则复合 $f = \beta \circ \varphi: I \to A$ 满足 $f(i) = \beta(\varphi(i)) = \beta(X_i) \in X_i$，因此它是 $\prod_{i \in I} X_i$ 的元素．所以笛卡儿积非空．

反之，设 A 是非空集合．定义 $I = \mathcal{P}(A)^{\#}$，考虑 $\prod_{S \in I} S$. 根据假设，这个积非空，因此它包含一个元素 β，其中对一切 $S \in \mathcal{P}(A)^{\#}, \beta(S) \in S$，即 β 是关于 A 的选择函数．所以选择公理成立．

■

选择公理有应用起来更方便的各种不同的等价形式，其中最普遍的是良序原则和佐恩引理，在给出以下预备定义之后我们再对它们进行陈述．大多数数学家接受选择公理（和我们一样），所以他们也接受那些等价形式．

回忆集合 X 是偏序集，如果存在定义在 X 上的自反的、反对称的和传递的关系 $x \leq y$. 如果有必要注明序关系，我们可以说 $(X, \leq)$ 是一个偏序集．

定义　设 X 是偏序集，如果 X 的每个非空子集 S 包含一个**最小元素**；即存在 $s_0 \in S$ 使得

$$\text{对一切 } s \in S, s_0 \leq s,$$

则称 X 为**良序**的．如果偏序集 X 中的任意两个元素都可比较；即对一切 $x, y \in X$，或者 $x \leq y$，或者 $y \leq x$，则称 X 为**链**．

⊖ 根据定义，一个集合 X 非空，如果存在元素 $x \in X$. 如果 $X_1 \neq \varnothing$ 和 $X_2 \neq \varnothing$，则存在 $x_1 \in X_1$ 和 $x_2 \in X_2$，因此 $(x_1, x_2) \in X_1 \times X_2$，即 $X_1 \times X_2 \neq \varnothing$. 一般来说，我们可以用归纳法证明，如果集合 $I = \{1, 2, \cdots, n\}$ 是有限的，则 $\prod_{i \in I} X_i = X_1 \times \cdots \times X_n \neq \varnothing$．于是，只有当指标集 I 无限时，选择公理才是重要的．

例 A.2 （ⅰ） 第1章中的最小整数公理说自然数N是良序集．一般地，N^n 配置以第6章中定义的单项序是良序集．

（ⅱ）空集$\varnothing$是良序集；否则，$\varnothing$将包含一个（没有最小元素的）非空子集，这是一个矛盾．

（ⅲ）整数Z不是良序集，因为没有最小整数．

（ⅳ）定义Q的子集 X 为

$$X=\{1-\frac{1}{n}:n\geqslant 1\}\cup\{2-\frac{1}{n}:n\geqslant 1\},$$

则 X 是良序集．注意 $1=2-\frac{1}{1}$ 有无限个前导．

（ⅴ）设 X 是良序集．称元素 $\tau\in X$ 是**顶元素**，如果不存在 $\alpha\in X$ 满足 $\tau\prec\alpha$. 如果 $\alpha\in X$ 不是 X 的顶元素（必须存在），则 $X^\alpha=\{\beta\in X:\alpha\prec\beta\}\neq\varnothing$，从而它有最小元素 α'，叫做 α 的**后继**. 后继 α' 是 α 之后的“下一个”元素：正式地说．$\alpha\prec\alpha'$，且没有 $\beta\in X$ 能够满足 $\alpha\prec\beta\prec\alpha'$（如果存在这样的 β，则 $\beta\in X^\alpha$，从而 $\alpha'\preceq\beta$). 如果元素 $\beta\in X$ 不是一个后继；即不存在 $\alpha\in X$ 使得 $\beta=\alpha'$，则称 β 是一个**极限**. X 的最小元素是一个极限；在（ⅳ）中，我们看到 $X=\{1-\frac{1}{n}:n\geqslant 1\}\cup\{2-\frac{1}{n}:n\geqslant 1\}$ 是良序集，显然 $1=2-\frac{1}{1}$ 是 X 中的一个极限．于是，X 中的每个元素或者是后继，或者是极限． ■

下面是良序集的几个基本性质．

命题 A.3 （ⅰ） *良序集 X 的每个子集 Y 也是良序集．*

（ⅱ）设 X 是良序集．如果 $x,y\in X$，则 $x\preceq y$ 或 $y\preceq x$.

（ⅲ）如果 X 是良序集，则 X 中的每个严格递减序列 $x_1\succ x_2\succ\cdots$ 是有限的．

（ⅳ）假定选择公理成立，（ⅲ）的逆为真．如果 X 是链，其中每个递减序列 $x_1\succ x_2\succ\cdots$ 都是有限的，则 X 是良序集．

证明 （ⅰ）如果 S 是 Y 的非空子集，则它也是 X 的子集，并且和 X 的任意非空子集一样，它包含最小元素．所以 Y 是良序集．

（ⅱ）子集 $S=\{x,y\}$ 有最小元素，它或者是 x，或者是 y. 在第一种情形，$x\preceq y$，在第二种情形，$y\preceq x$.

（ⅲ）如果 X 是良序集，则 $S=\{x_1,x_2,\cdots\}$ 有最小元素，比如 x_i；即对一切 $n\geqslant 1,x_n\succeq x_i$. 特别地，如果 $n=i+1$,则 $x_{i+1}\succeq x_i$,与 $x_i\succ x_{i+1}$ 矛盾．

（ⅳ）假定存在 X 的非空子集 S，它没有最小元素．选取 $s_0\in S$；因 s_0 不是最小的，所以对一切 $s\in S,s_0\preceq s$ 不真．于是，不是存在 $s_1\in S$ 使得 $s_0\succ s_1$，就是有 $s\in S$ 使得 s_0 和 s 不可比较；后一种情况不可能发生，因为 X 是链．类似地，存在 $s_2\in S$ 使得 $s_1\succ s_2$. 由归纳法，对一切 $n\geqslant 0$，存在元素 $s_i\in S$ 使得 $s_0\succ s_1\succ\cdots\succ s_n\succ s_{n+1}$. 我们要集中这无限个选取，对每个 n 选取一个，形成一个递减序列[⊖]；即要有一个函数 $f:N\to S$ 使得 $f(n)=s_n$. 下面是正式做法．设$\mathcal{F}$是来自一切初始段 $\{0,1,\cdots,n\}\to S$ 的一切函数 g 的族，并设 β 是$\mathcal{F}$上的选择函数：即对每个非空子集 $T\subseteq\mathcal{F},\beta(T)\in T$. 我们用 β 来构造所要的序列．

选取一个元素 $s_0\in S$，这是可能的，因为 $S\neq\varnothing$. 定义 $F_0=\{g\in\mathcal{F}$ ：定义域 $(g)=\{0\}$ 且 $g(0)=s_0\}$

⊖ 在命题 6.38 中证明 ACC 蕴涵极大条件时我们已经这样做了，没有加以注释．事实上，那个证明只用了选择公理的一个较弱的形式，即指标集是可数的．

(在 F_0 中只有一个函数 g)，并定义 $g_0=\beta(F_0)$. 对 $n>0$，由归纳法可知 $F_{n+1}\neq\varnothing$，其中

$$F_{n+1}=\{g:\{0,1,\cdots,n+1\}\to X:g\mid\{0,\cdots,n\}=g_n \text{ 且 } g(n)>g(n+1)\}.$$

所以，可以定义 $g_{n+1}=\beta(F_{n+1})$. 最后，定义 g^* 为 g_n 的并；即对一切 $n, g^*(n)=g_n(n)$. 函数g^*是 S 中的严格递减序列，与假设 S 中的每个严格递减序列是有限的矛盾. ■

良序原则 每个集合 X 都有它的元素的某个良序.

如果 X 正好是一个偏序集，则良序原则断言必存在一个良序，而这个良序可能与原来的偏序无关. 例如，$\mathbb{Z}$ 可这样良序化：

$$0\preceq 1\preceq -1\preceq 2\preceq -2\preceq\cdots.$$

$\mathbb{N}$ 是良序的，这正是陈述数学归纳法的另一种方法. 于是良序原则提出了一种广义归纳法的可行性，它应用于以良序集加标的一族陈述，该良序集可以有任意（可以不可数）基数. 事实上，这样的推广确实是存在的，叫做**超穷归纳法**. 设 $\{S(\alpha):\alpha\in I\}$ 是以良序集 I 加标的一族陈述. 如果 α_0 是 I 中的最小指标，则基础步是 $S(\alpha_0)$ 为真的陈述. 归纳步是如下的陈述：如果 β 是一个指标，且对一切 $\alpha<\beta, S(\alpha)$ 为真，则 $S(\beta)$ 为真. 超穷归纳法说，如果基础步和归纳步成立，则一切陈述 $S(\alpha)$ 都真.（通常，归纳步的证明分作两种情形，这依赖于 β 是一个后继还是一个极限）. 这里有一个应用超穷归纳法的令人惊奇的结果：存在平面的子集 Q，它和每条直线恰好交于两个点. 证明的思想是用平面中一切直线的良序集来构造 Q，要求每条直线只有可数个前导. 现在从每条直线上依次审慎地选出最多两个点放进 Q 中.

在下面的定义之后我们就能够陈述佐恩引理.

定义 设 X 是偏序集. X 的子集 S 的一个**上界**是指元素 $x\in X$，不必在 S 中，满足

$$\text{对一切 } s\in S, s\preceq x.$$

如果对于元素 $m\in X$，没有 $x\in X$ 满足 $m\prec x$；即如果 $x\in X$ 且 $m\preceq x$，则 $m=x$，则称 m 为一个**极大元素**.

一个偏序集可以没有极大元素：例如$\mathbb{R}$ 在通常序下是一个链，它没有极大元素. 一个偏序集也可以有很多极大元素：例如，如果 X 是集合 U 的一切真子集构成的偏序集，则子集 S 是极大元素当且仅当有某个 $u\in U$ 使得 $S=U-\{u\}$；即 S 是一个点的补集.

佐恩引理是保证极大元素存在的准则.

佐恩引理 如果 X 是非空偏序集，其中每个链都有一个上界，则 X 有极大元素.

定理 A.4 下列陈述等价：

（ⅰ）佐恩引理.

（ⅱ）良序原则.

（ⅲ）选择公理.

我们把定理 A.4 分裂为三个定理. 下面先从一个定义和一个引理开始.

定义 如果 X 是良序集且 $c\in X$，则**开前段**$\mathrm{Seg}(c)$是指子集

$$\mathrm{Seg}(c)=\{x\in X:x\prec c\}.$$

下面的结果补充了命题 A.3.

引理 A.5 链 X 是良序的当且仅当 X 的每个开前段是良序的.

证明 必要性是显然的，因为良序集的每个子集是良序的. 反之，设 S 是 X 的非空子集. 当然，如果 S 是单元素集，则它包含最小元素，因此可以假定 S 至少包含两个元素，比如 c'和 c. 因

X 是链，可以假定 $c' \prec c$. 因此 $\mathrm{Seg}(c) \cap S \neq \varnothing$；由于良序集的每个非空子集是良序的，在 $\mathrm{Seg}(c) \cap S$ 中存在最小元素，比如 z. 现在 z 也是 S 中的最小元素，这是因为如果有 $s' \in S$ 使得 $s' \prec z$，则 $s' \in \mathrm{Seg}(c) \cap S$，与 z 是 $\mathrm{Seg}(c) \cap S$ 中的最小元素矛盾．所以 X 是良序的． ■

一般来说，一个偏序集的良序子集的递增的并未必是良序的．例如，易知对每个正整数 n，子集

$$S_n = \{m \in \mathbb{Z} : m \geqslant -n\}$$

是 $\mathbb{Z}$ 的良序子集，但 $\bigcup_n S_n = \mathbb{Z}$ 不是良序的．

添加一个额外的假设，我们可以迫使良序子集的并也是良序的．

记号 如果 B 和 C 都是偏序集 X 的子集，则用

$$B \trianglelefteq C$$

表示 $B = C$ 或 B 是 C 的一个开前段；即存在 $c \in C$ 使得 $B = \mathrm{Seg}(c)$.

引理 A.6 设 $(X, \preceq)$ 是偏序集，并设 $\{S_i : i \in I\}$ 是以集合 I 加标的 X 的一族良序子集．如果对每个 i, j，不是 $S_i \trianglelefteq S_j$ 就是 $S_j \trianglelefteq S_i$，则 $\bigcup_{i \in I} S_i$ 是 X 的良序子集．

证明 设 $U = \bigcup_i S_i$. 根据引理 A.5，只需证明任意开前段 $\mathrm{Seg}(c)$ 是良序的，其中 $c \in U$. 现在有某个 i 使得 $c \in S_i$；因 S_i 是良序的，从而它的任意子集也是良序的；于是只需证明 $\mathrm{Seg}(c) = \{u \in U : u \prec c\} \subseteq S_i$；即如果 $u \prec c$，我们需要证明 $u \in S_i$. 现在有某个 j 使得 $u \in S_j$. 如果 $S_j \trianglelefteq S_i$，则 $u \in S_i$，结果已经得到．如果 $S_i \trianglelefteq S_j$，则 $S_i \subseteq S_j$，从而 $c \in S_j$；此外，因 S_i 是 S_j 是开前段，$u \prec c$ 蕴涵 $u \in S_i$，正如所求． ■

定义 如果良序集 $(X, \preceq)$ 的子集 A 满足 $A \neq \varnothing$，且 $x \preceq a$ 蕴涵 $x \in A$，其中 $x \in X$ 和 $a \in A$，则称子集 A 在 X 中是闭的．(于是，如果 A 是闭的和 $a \in A$，则 A 包含每个比 a 小的元素．)

给定一个良序集 X 和 $c \in X$，显然“闭前段”

$$A = \{x \in X : x \preceq c\}$$

是闭子集．如果 c 是 X 的顶元素（应该存在），则 $A = X$；如果 c 不是顶元素，则它有后继 c'，且 $A = \mathrm{Seg}(c')$. 于是，闭前段是闭子集，但不是什么新东西．

引理 A.7 如果 $(X, \preceq)$ 是良序集，则 A 在 X 中是闭的当且仅当 $A \trianglelefteq X$；即不是 $A = X$ 就是有某个 $c \in X$ 使得 $A = \mathrm{Seg}(c)$.

证明 显然开前段是闭的，从而只有必要性需要证明．

假定 A 是闭的；我们需要证明如果 $A \neq X$，则 A 是一个开前段．因 X 是良序的，有最小元素 $c \in X - A$，我们断言 $A = \mathrm{Seg}(c)$. 如果有某个 $a \in A$ 使得 $c \preceq a$，则因 A 是闭的，必有 $c \in A$，与 $c \notin A$ 矛盾．所以对一切 $a \in A$，$a \prec c$（我们用了良序集是链的事实）；即 c 是 A 的上界，因此 $A \subseteq \mathrm{Seg}(c)$. 关于反包含，假设 $x \in \mathrm{Seg}(c)$；即 $x \prec c$. 如果 $x \notin A$，则 $x \in X - A$，从而 $c \preceq x$，产生矛盾． ■

下面是定理 A.4 的第一步．

定理 A.8 如果佐恩引理成立，则良序原则成立：每个集合 X 都可良序化．

证明 因 $\varnothing$ 是良序的，可以假定 $X \neq \varnothing$. 设 $\mathcal{L}$ 是 X 的一切良序子集的族；精确地说，$\mathcal{L}$ 的元素是一个有序对 $(S, \sqsubseteq)$，它由 X 的子集 S 和它的某个良序 $\sqsubseteq$ 组成．于是，X 的子集可以在 $\mathcal{L}$ 中出现几次，配置以不同的良序．我们现在把 $\mathcal{L}$ 做成一个偏序集．定义

$$(S, \sqsubseteq) \preceq (S', \sqsubseteq')$$

表示或者（i）$S=S'$ 和$\sqsubseteq=\sqsubseteq'$ 或者（ii）$S\subsetneq S'$，在 S 上序一致（即如果 $a,b\in S$，则 $a\sqsubseteq b$ 成立当且仅当 $a\sqsubseteq' b$ 成立），且 S 是 S' 的开前段．

我们现在证明$\mathcal{L}$满足佐恩引理的假设．注意因任意 1-点子集是良序集，从而给出$\mathcal{L}$的一个元素，所以 $\mathcal{L}\neq\varnothing$．设 $C=\{(S_i,\preceq_i):i\in I\}$ 是$\mathcal{L}$中的一个链；即对每个 i,j，或者 $(S_i,\sqsubseteq_i)\preceq(S_j,\sqsubseteq_j)$，或者 $(S_j,\sqsubseteq_j)\preceq(S_i,\sqsubseteq_i)$．定义 $U=\bigcup_i S_i$，并定义 U 上的偏序$\sqsubseteq$如下．如果 $u,v\in U$，则存在指标 i 和 j 使得 $u\in S_i$ 和 $v\in S_j$；可以假定$(S_i,\sqsubseteq_i)\preceq(S_j,\sqsubseteq_j)$，从而 $u,v\in S_j$．如果 $u\sqsubseteq_j v$，我们定义 $u\sqsubseteq v$．这个定义不依赖于指标的选取，这是因为如果有指标 k 和 ℓ 使得 $u\in S_k$ 和 $v\in S_\ell$，则$(S_k,\sqsubseteq_k)\preceq(S_\ell,\sqsubseteq_\ell)$ 和 $u\sqsubseteq_\ell v$ 是和原来的定义相竞争的定义．但 $(S_j,\sqsubseteq_j)\preceq(S_\ell,\sqsubseteq_\ell)$，从而 $u\sqsubseteq_j v$ 当且仅当 $u\sqsubseteq_\ell v$．现在容易证明$(U,\sqsubseteq)$ 是偏序集．事实上，根据引理 A.6，$(U,\sqsubseteq)$ 是良序集，从而 $(U,\sqsubseteq)\in\mathcal{L}$．我们进一步断言每个 $(S_i,\sqsubseteq_i)$ 在 $(U,\sqsubseteq)$ 中是闭的．假定 $u\sqsubseteq s_i$，其中 $s_i\in S_i$ 和 $u\in U$．现在有某个 j 使得 $u\in S_j$；如果 $(S_j,\sqsubseteq_j)\preceq(S_i,\sqsubseteq_i)$，则正如所要的有 $u\in S_i$；如果 $(S_i,\sqsubseteq_i)\preceq(S_j,\sqsubseteq_j)$，则 S_i 在 S_j 中是闭的，从而 $u\in S_i$．现在引理 A.7 给出，对一切 i，$(S_i,\sqsubseteq_i)\preceq(U,\sqsubseteq)$；即$(U,\sqsubseteq)$是 C 的上界．

根据佐恩引理，$\mathcal{L}$有极大元素，比如 $(M,\leqslant)$．如果 M 包含 X 的每个元素，则 X 是良序集．如果存在某个 $x\in X$ 且 $x\notin M$，则定义 $M\cup\{x\}$ 的良序$\leqslant'$是给定的 M 的良序的扩张，对每个 $m\in M$ 定义 $m<'x$．因在 $M\cup\{x\}$ 中 $M=\mathrm{Seg}(x)$，所以有 $(M,\leqslant)\prec(M\cup\{x\},\leqslant')$，与 $(M,\leqslant)$ 的极大性矛盾．所以 $M=X$ 及 X 可以良序化． ■

涉及佐恩引理的几乎所有证明都有同样的格式：定义一个合适的非空偏序集；证明它的链有上界；证明由佐恩引理保证存在的极大元素能够用来求证定理（最后一步常用间接证法）．

在呈示定理 A.4 的第二步证明之前，关于选择公理有一个小注释．给定集合 A 和 X，定义函数 $f:A\to X$ 的一种方法是指定它的值．例如，存在函数 $f:\mathbb{N}\to\mathbb{N}$ 使得对每个 $n\in\mathbb{N}$，$f(n)=n+1$．然而，不是每个函数都由一个公式给出，选择公理处理一个函数什么时候被确实定义的问题．如果 $\{G_a:a\in A\}$ 是一族群，则可以定义选择函数 $f:A\to\bigcup_a G_a$ 为 $f(a)=1_a$，其中 1_a 是 G_a 的幺元；我们不需要用选择公理来定义 f．与之相比，如果仅仅"选取"某个元素 $x_a\in G_a$，则"函数" $h:A\to\bigcup_a G_a$ 使得 $h(a)=x_a$ 不是合理定义的．这样的"函数"应该不是一个真实的函数．如何发觉 h 的某种性质；例如 h 是单射吗？

定理 A.9 *良序原则蕴涵选择公理．*

证明 设 A 是非空集合．我们可以假定 A 的元素有某个良序，由此 A 的每个非空子集也是良序的．定义一个选择函数 $\beta:\mathcal{P}(A)^\#\to A$ 为对 A 的每个非空子集 S，$\beta(S)$ 为 S 的最小元素． ■

Daniel Grayson 告诉我选择公理蕴涵佐恩引理的一个精致的证明；它不同于 1904 年 E. Zermelo 的证明以及 1950 年 H. Kneser 的修改．

定理 A.10 *选择公理蕴涵佐恩引理．*

证明 假定 X 没有极大元素．如果 A 是 X 的良序子集，则 A 是链，因此 A 有上界，比如 x．因 x 不是极大元素，存在 $y\in X$ 使得 $x\prec y$；由此每个良序子集 A 有不在 A 中的上界．令$\mathcal{W}$表示 X 的一切良序子集的族．对每个 $A\in\mathcal{W}$，定义

$$U_A=\{A\text{ 的一切上界 }u\text{ 满足 }u\notin A\};$$

根据假设每个$U_A \neq \varnothing$，从而命题 A.1 说存在某个g在$\prod_{A\in\mathcal{W}} U_A$中．于是对一切$A\in\mathcal{W}$，有$A$的一个上界$g(A)$且$g(A)\notin A$.

我们用g来构造一些特定的良序子集．定义元素$c_0\in X$为$c_0=g(\varnothing)$．称X的一个良序子集C为**g-集**，如果c是被g选取的$C\cap \mathrm{Seg}(c)$的上界；[⊖]即$c_0\in C$且对每个$c\in C, c=g(C\cap \mathrm{Seg}(c))$.

我们要证明一切g-集的并也是一个g-集，然后证明这导致一个矛盾．

如果C和D都是g-集．我们断言或者$C\trianglelefteq D$或者$D\trianglelefteq C$. 定义W为满足$B\trianglelefteq C$和$B\trianglelefteq D$的一切子集B的并．我们断言$W\trianglelefteq C$和$W\trianglelefteq D$；即W在C中和在D中都是闭的．取$w\in W$；这个元素所以在W中是因为它在某个B中，其中$B\trianglelefteq C$和$B\trianglelefteq D$. 如果$c\in C$和$c\preceq w$，则$c\in B$（因为B在C中是闭的）．因此，$c\in B\subseteq W$（因为根据定义，W是一切这种子集B的并）．所以W在C中是闭的．类似地，W在D中是闭的．如果$W=C$或$W=D$，则断言为真．因此可以假定$W\lhd C$［从而有某个$c'\in C-W$使得$W=C\cap \mathrm{Seg}(c')$］和$W\lhd D$［从而有某个$d'\in D-W$使得$W=D\cap \mathrm{Seg}(d')$］. 因C和D都是g-集，$c'=g(C\cap \mathrm{Seg}(c'))=g(W)$和$d'=g(D\cap \mathrm{Seg}(d'))=g(W)$. 所以，$c'=d'$. 但现在$W\cup\{c'\}=W\cup\{d'\}$在$C$中和在$D$中都是闭的，这是因为它是一个闭区间．于是$W\cup\{c'\}\subseteq W$，与$c'\notin W$矛盾．所以$W=C$或$W=D$；即如所断言的那样，或者$C\trianglelefteq D$，或者$D\trianglelefteq C$.

最后，设Ω是一切g-集的并．刚建立的断言证明满足引理 A.6 的假设，从而Ω是良序子集．我们证明Ω自身是一个g-集．如果$c\in\Omega$，则存在某个g-集C包含c，且$c=g(C\cap \mathrm{seg}(c))$. 但根据引理 A.7 和上面刚证明的或者$C\trianglelefteq\Omega$或者$\Omega\trianglelefteq C$的事实，有$C\trianglelefteq\Omega$；因此$C\cap \mathrm{seg}(c)=\Omega\cap \mathrm{Seg}(c)$. 所以，$c=g(\Omega\cap \mathrm{seg}(c))$，从而$\Omega$是一个$g$-集．另一方面，$\Omega'=\Omega\cup\{g(\Omega)\}$是不包含在$\Omega$中的$g$-集，这是一个矛盾．由此可知这样的函数$g$不存在，因此$X$有极大元素． ■

这个证明表明我们只用了一个比佐恩引理的证明较弱的假设：只需良序子集有上界．然而，习题 6.45 证明偏序集中的每个链C包含一个良序子集W使得C和W有相同的上界．因此，如果一切良序子集都有上界，则所有的链也有上界．

[⊖] 下面每个集合都是g-集．如果$c_1=g(\{c_0\})$，定义$c_2=g(\{c_0,c_1\})$，并归纳定义$c_{n+1}=g(\{c_0,\cdots,c_n\})$. 注意$c_0\prec c_1\prec c_2\prec\cdots$. 每个子集$\{c_0,c_1,\cdots,c_n\}$是$g$-集．也存在无限的$g$-集．例如，如果$C'=\{c_n: n\in \mathrm{N}\}$，令$c'=g(C')$，并定义$C''=C'\cup\{c'\}$.

参考文献

Adem, A., and Milgram, R. J., *Cohomology of Finite Groups*, Springer-Verlag, Berlin, 1994.

Albert, A. A., editor, *Studies in Modern Algebra*, MAA Studies in Mathematics, vol. 2, Mathematical Association of America, Washington, 1963.

Artin, E., *Geometric Algebra*, Interscience Publishers, New York, 1957.

Artin, E., Nesbitt, C. J., and Thrall, R. M., *Rings with Minimum Condition*, University of Michigan Press, Ann Arbor, 1968.

Aschbacher, M., *Finite Group Theory*, Cambridge University Press, Cambridge, 1986.

Atiyah, M., and Macdonald, I. G., *Introduction to Commutative Algebra*, Addison-Wesley, Reading, 1969.

Biggs, N. L., *Discrete Mathematics*, Oxford University Press, 1989.

Birkhoff, G., and Mac Lane, S., *A Survey of Modern Algebra*, 4th ed., Macmillan, New York, 1977.

Blyth, T. S., *Module Theory; an Approach to Linear Algebra*, Oxford University Press, 1990.

Borevich, Z. I., and Shafarevich, I. R., *Number Theory*, Academic Press, Orlando, 1966.

Bourbaki, N., *Elements of Mathematics; Algebra* I; *Chapters* 1-3, Springer-Verlag, New York, 1989.

———, *Elements of Mathematics; Commutative Algebra*, Addison-Wesley, Reading, 1972.

Brown, K. S., *Cohomology of Groups*, Springer-Verlag, Berlin, 1982.

Bruns, W., and Herzog, J., *Cohen-Macaulay Rings*, Cambridge University Press, 1993.

Buchberger, B., and Winkler, F., editors, *Gröbner Bases and Applications*, LMS Lecture Note Series 251, Cambridge University Press, 1998.

Burnside, W., *The Theory of Groups of Finite Order*, 2d ed., Cambridge University Press, 1911; Dover reprint, Mineola, 1955.

Caenepeel, S., *Brauer Groups, Hopf Algebras, and Galois Theory*, Kluwer, Dordrecht, 1998.

Cajori, F., *A History of Mathematical Notation*, Open Court, 1928; Dover reprint, Mineola, 1993.

Carmichael, R., *An Introduction to the Theory of Groups*, Ginn, New York, 1937.

Carter, R., *Simple Groups of Lie Type*, Cambridge University Press, Cambridge, 1972.

Cassels, J. W. S., and Fröhlich, A., *Algebraic Number Theory*, Thompson Book Co., Washington, D.C., 1967.

Conway, J. H., Curtis, R. T., Norton, S. P., Parker, R. A., Wilson, R. A., *ATLAS of Finite Groups*, Oxford University Press, 1985.

Cox, D., Little, J., and O'Shea, D., *Ideals, Varieties, and Algorithms*, 2d ed., Springer-Verlag, New York, 1997.

Coxeter, H. S. M., and Moser, W. O. J., *Generators and Relations for Discrete Groups*, Springer-Verlag, New York, 1972.

Curtis, C. W., and Reiner, I., *Representation Theory of Finite Groups and Associative Algebras*, Interscience, New York, 1962.

Dieudonné, J., *La Géometrie des Groupes Classiques*, Springer-Verlag, Berlin, 1971.

Dixon, J. D., du Sautoy, M. P F., Mann, A., and Segal, D., *Analytic Pro-p Groups*, Cambridge University Press, 1991.

Dornhoff, L., *Group Representation Theory*, *Part* A, *Ordinary Representation Theory*, Marcel Dekker, New York, 1971.

Drozd, Yu. A., and Kirichenko, V. V., *Finite Dimensional Algebras*, Springer-Verlag, New York, 1994.

Dummit, D. S., and Foote, R. M., *Abstract Algebra*, 2nd ed., Prentice Hall, Upper Saddle River, 1999.

Eisenbud, D., *Commutative Algebra with a View Toward Algebraic Geometry*, Springer- Verlag, New York, 1995.

Evens, L., *The Cohomology of Groups*, Oxford Mathematical Monographs, Oxford University Press, New York, 1991.

Farb, B., and Dennis, R. K., *Noncommutative Algebra*, Springer-Verlag, New York, 1993.

Feit, W., *Characters of Finite Groups*, W. A. Benjamin, New York, 1967.

Fröhlich, A., and Taylor, M. J., *Algebraic Number Theory*, Cambridge Studies in Advanced Mathematics 27, Cambridge University Press, 1991.

Fuchs, L., *Infinite Abelian Groups* I, Academic Press, Orlando, 1970.

———, *Infinite Abelian Groups* II, Academic Press, Orlando, 1973.

Fulton, W., *Algebraic Curves*, Benjamin, New York, 1969.

———, *Algebraic Topology; A First Course*, Springer-Verlag, New York, 1995.

Gaal, L., *Classical Galois Theory with Examples*, 4th ed., Chelsea, American Mathematical Society, Providence, 1998.

Gorenstein, D., Lyons, R. and Solomon, R., *The Classification of the Finite Simple Groups*, Math. Surveys and Monographs Volume 40, American Mathematical Society, Providence, 1994.

Greub, W. H., *Multilinear Algebra*, Springer-Verlag, New York, 1967.

Hadlock, C., *Field Theory and Its Classical Problems*, Carus Mathematical Monographs, Mathematical Association of America, Washington, 1978

Hahn, A. J., *Quadratic Algebras, Clifford Algebras, and Arithmetic Witt Groups*, Universitext, Springer-Verlag, New York, 1994.

Hardy, G. H., and Wright, E. M., *An Introduction to the Theory of Numbers*, 4th ed., Oxford University Press, 1960.

Harris, J., *Algebraic Geometry*, Springer-Verlag, New York, 1992.

Hartshorne, R., *Algebraic Geometry*, Springer-Verlag, New York, 1977.

Herstein, I. N., *Topics in Algebra*, 2d ed., Wiley, New York, 1975.

———, *Noncommutative Rings*, Carus Mathematical Monographs No. 15, Mathematical Association of America, Washington, 1968.

Humphreys, J. E., *Introduction to Lie Algebras and Representation Theory*, Springer- Verlag, New York, 1972.

Huppert, B., *Character Theory of Finite Groups*, de Gruyter, Berlin, 1998.

———, *Endliche Gruppen* I, Springer-Verlag, New York, 1967.

Isaacs, I. M., *Character Theory of Finite Groups*, Academic Press, San Diego, 1976.

———, *Algebra, A Graduate Course*, Brooks/Cole Publishing, Pacific Grove, 1994.

Jacobson, N., *Basic Algebra* I, Freeman, San Francisco, 1974.

———, *Basic Algebra* II, Freeman, San Francisco, 1980.

———, *Finite-Dimensional Division Algebras over Fields*, Springer-Verlag, New York, 1996.

———, *Lie Algebras*, Interscience Tracts Number 10, Wiley, New York, 1962.

———, *Structure of Rings*, Colloquium Publications 37, American Mathematical Society, Providence, 1956.

Kaplansky, I., *Commutative Rings*, University of Chicago Press, 1974.

———, *Fields and Rings*, 2d ed., University of Chicago Press, 1972.

———, *Infinite Abelian Groups*, University of Michigan Press, Ann Arbor, 1969.

———, *Linear Algebra and Geometry; a Second Course*, Allyn& Bacon, Boston, 1969.

———, *Set Theory and Metric Spaces*, Chelsea, American Mathematical Society, Providence, 1977.

Kostrikin, A. I., and Shafarevich, I. R. (editors), *Encyclopaedia of Mathematical Sciences, Algebra* IX: *Finite Groups of Lie Type: Finite-Dimensional Division Algebras*, Springer-Verlag, New York, 1996.

Lam, T. Y, *The Algebraic Theory of Quadratic Forms*, Benjamin, Reading, 1973, 2d. revised printing, 1980.

———, *A First Course in Noncommutative Rings*, Springer-Verlag, New York, 1991.

———, *Lectures on Modules and Rings*, Springer-Verlag, New York, 1999.

Lang, S., *Algebra*, 3d ed., Addison-Wesley, Reading, 1993.

Lidl, R., and Niederreiter, H., *Introduction to Finite Fields and Their Applications*, University Press, Cambridge, 1986.

Lyndon, R. C., and Schupp, P. E., *Combinatorial Group Theory*, Springer-Verlag, New York, 1977.

Macdonald, I. G., *Algebraic Geometry; Introduction to Schemes*, Benjamin, New York, 1968.

Mac Lane, S., *Categories for the Working Mathematician*, Springer-Verlag, New York, 1971.

———, *Homology*, Springer-Verlag, New York, 3d corrected printing, 1975.

Mac Lane, S., and Birkhoff, G., *Algebra*, MacMillan, New York, 1967.

Malle, G., and Matzat, B., *Inverse Galois Theory*, Springer-Verlag, New York, 1999.

Matsumura, H., *Commutative Ring Theory*, Cambridge University Press, 1986.

McCleary, J., *User's Guide to Spectral Sequences*, Publish or Perish, Wilmington, 1985.

McConnell, J. C., and Robson, J. C., *Noncommutative Noetherian Rings*, Wiley, New York, 1987.

McCoy, N. H., and Janusz, G. J., *Introduction to Modern Algebra*, 5th ed., Wm. C. Brown Publishers, Dubuque, Iowa, 1992.

Milnor, J., *Introduction to Algebraic K-Theory*, Annals of Mathematical Studies, No. 72, Princeton University Press, 1971.

Montgomery, S. and Ralston, E. W., *Selected Papers on Algebra*, Raymond W. Brink Selected Mathematical Papers, volume 3, Mathematical Association of America, Washington, 1977.

Mumford, D., *The Red Book of Varieties and Schemes*, Lecture Notes in Mathematics 1358, Springer-Verlag, New York, 1988.

Neukirch, J., Schmidt, A., and Wingberg, K., *Cohomology of Number Fields*, Grundlehren der mathematicshcen Wissenschaften, vol. 323, Springer-Verlag, New York, 2000.

Niven, I., and Zuckerman, H. S., *An Introduction to the Theory of Numbers*, Wiley, New York, 1972.

Northcott, D. G., *Ideal Theory*, Cambridge University Press, 1953.

O'Meara, O. T., *Introduction to Quadratic Forms*, Springer-Verlag, New York, 1971.

Orzech, M., and Small, C., *The Brauer Group of Commutative Rings*, Lecture Notes in Pure and Applied Mathematics, Marcel Dekker, New York, 1975.

Pollard, H., *The Theory of Algebraic Numbers*, Carus Mathematical Monograps Number 9, Mathematical Association of America, 1950.

Procesi, C., *Rings with Polynomial Identities*, Marcel Dekker, New York, 1973.

Reiner, I., *Maximal Orders*, Academic Press, London, 1975; Oxford University Press, 2003.

Robinson, D. J. S., *A Course in the Theory of Groups*, 2d ed., Springer-Verlag, New York, 1996.

Rosenberg, J., *Algebraic K-Theory and Its Applications*, Springer-Verlag, New York, 1994.

Rotman, J. J., *A First Course in Abstract Algebra*, 2d ed., Prentice Hall, Upper Saddle River, 2000.

———, *Galois Theory*, 2d ed., Springer-Verlag, New York, 1998.

———, *An Introduction to Homological Algebra*, Academic Press, Orlando, 1979.

———, *An Introduction to the Theory of Groups*, 4th ed., Springer-Verlag, New York, 1995.

———, *Journey into Mathematics*, Prentice Hall, Upper Saddle River, 1998.

Rowen, L. H., *Polynomial Identities in Ring Theory*, Academic Press, New York, 1980.

Samuel, P. *Algebraic Theory of Numbers*, Houghton Mifflin, Boston, 1970.

Serre, J.-P., *Algèbre Locale: Multiplicités*, Lecture Notes in Mathematics 11, 3d ed., Springer-Verlag, New York, 1975.

———, *Corps Locaux*, Hermann, Paris, 1968.

———, *Trees*, Springer-Verlag, New York, 1980.

Sims, C. C., *Computation with Finitely Presented Groups*, Cambridge University Press, 1994.

Stillwell, J. , *Mathematics and Its History*, Springer-Verlag, New York, 1989.

Suzuki, M. , *Group Theory* I, Springer-Verlag, New York, 1982.

Tignol, J.-P. , *Galois'Theory of Algebraic Equations*, Wiley, New York, 1988; World Scientific, Singapore, 2001.

van der Waerden, B. L. , *Geometry and Algebra in Ancient Civilizations*, Springer-Verlag, New York, 1983.

————, *A History of Algebra*, Springer-Verlag, New York, 1985.

————, *Modern Algebra*, 4th ed. , Ungar, New York, 1966.

————, *Science Awakening*, Wiley, New York, 1963.

Weibel, C. , *An Introduction to Homological Algebra*, Cambridge University Press, 1994.

Weyl, H. , *The Classical Groups; Their Invariants and Representations*, Princeton, 1946.

Weiss, E. , *Cohomology of Groups*, Academic Press, Orlando, 1969.

Zariski, O. , and Samuel, P. , *Commutative Algebra* I, van Nostrand, Princeton, 1958.

————, *Commutative Algebra* II, van Nostrand, Princeton, 1960.

索 引

索引中的页码为英文原书页码，与书中页边标注的页码一致．

A

C

D

E

F

G

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Y

Z